PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 02 May 2001 (02.05.01)	
International application No. PCT/JP00/05832	**Applicant's or agent's file reference** 900392
International filing date (day/month/year) 29 August 2000 (29.08.00)	**Priority date** (day/month/year) 30 August 1999 (30.08.99)
Applicant HATANAKA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

26 March 2001 (26.03.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Kiwa Mpay

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

FUKAMI, Hisao
Mitsui Sumitomo Bank
Minamimorimachi Bldg.
1-29, Minamimorimachi 2-chome,
Kita-ku
Osaka-shi, Osaka 530-0054
JAPON

Date of mailing (day/month/year)
17 July 2001 (17.07.01)

Applicant's or agent's file reference
900392

IMPORTANT NOTIFICATION

International application No.
PCT/JP00/05832

International filing date (day/month/year)
29 August 2000 (29.08.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address

1) FUKAMI, Hisao
2) MORITA, Toshio
3) HORII, Yutaka
Sumitomo Bank Minamimori-machi Building
1-29, Minamimori-machi 2-chome
Kita-ku, Osaka-shi
Osaka 530-0054
Japan

State of Nationality:
State of Residence:
Telephone No.: 06-6361-2021
Facsimile No.: 06-6361-1731
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address

1) FUKAMI, Hisao
2) MORITA, Toshio
3) HORII, Yutaka
Mitsui Sumitomo Bank Minamimorimachi Bldg.
1-29, Minamimorimachi 2-chome,
Kita-ku, Osaka-shi, Osaka 530-0054
Japan

State of Nationality:
State of Residence:
Telephone No.: 06-6361-2021
Facsimile No.: 06-6361-1731
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[X] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Shinji IGARASHI

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

004155929

10T

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 900392	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP00/05832	International filing date (*day month year*) 29 August 2000 (29.08.00)	Priority date (*day month year*) 30 August 1999 (30.08.99)
International Patent Classification (IPC) or national classification and IPC G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H 1/00, H04M 3/42, 3/493, 11/08, G10L 19/00		
Applicant FUJITSU LIMITED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 19 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
26 March 2001 (26.03.01)	17 September 2001 (17.09.2001)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP00/05832

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 4-35 . as originally filed
pages _____ . filed with the demand
pages 1-3.3/1-3/4 . filed with the letter of 20 June 2001 (20.06.2001)

☒ the claims:

pages _____ . as originally filed
pages _____ . as amended (together with any statement under Article 19
pages _____ . filed with the demand
pages 1-14 . filed with the letter of 20 June 2001 (20.06.2001)

☒ the drawings:

pages 1-22 . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☐ the sequence listing part of the description:

pages _____ . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP 00/05832

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-41	YES
	Claims		NO
Inventive step (IS)	Claims	1-41	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-41	YES
	Claims		NO

2. Citations and explanations

Claims 1-5

Document 1 (EP, 817185, A2 (Toshiba Corp.), 7 January 1998 (07.01.98)) and Document 2 ("Kogata memori kaado de ongaku chosakuken wo mamoru" [Protecting musical copyright with small memory cards], Nikkei Electronics, No. 739, 22 March 1999 (22.03.99), pp. 49-53) are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data storage component which stores a content key encrypted in a code which can be decrypted by a specific key in the data reproduction component.

Claims 6-11

Documents 1 and 2 are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data storage component which

encrypts a session key which is different for each access to obtain the content keys, using a code that can be decrypted by a specific key in the data reproduction component, and feeds this to the data reproduction component.

Claims 12-22 and 31-41

Documents 1 and 2 are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data storage component which a encrypts session key which is different for each access to obtain content data, using a code that can be decrypted by a specific key in the data reproduction component, and feeds this to the data reproduction component.

Claims 23-30

Documents 1 and 2 are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data reproduction module using a specific key for the data reproduction component and a session key encoded by a separate session key.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

In the description, page 36, line 12, the "session key generating component" is given the number "1520", but in Fig. 4, number "1520" is the "decrypting treatment component" and not the "session key generating component". Therefore, the number is not used consistently throughout the whole of the international application.

Similarly, in the description, page 36, lines 14-15, the "first encryption treatment component" is given the number "1540", but in Fig. 4, number "1540" is the "Kp holding component" and not the "first encryption treatment component". Therefore, the number is not used consistently throughout the whole of the international application.

EP・US　　特許協力条約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　９００３９２	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５８３２	国際出願日 （日.月.年）　２９．０８．００	優先日 （日.月.年）　３０．０８．９９
出願人（氏名又は名称） 富士通株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　2　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査[redacted]　　国際出願番[redacted]ＰＣＴ／ＪＰ００／０５８３２

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int Cl' Ｇ１０Ｋ１５／０２，Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１７／６０，Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／１０，
Ｇ０６Ｋ１９／００，Ｈ０４Ｈ１／００，Ｈ０４Ｍ３／４２，Ｈ０４Ｍ３／４９３，Ｈ０４Ｍ１１／０８，
Ｇ１０Ｌ１９／００

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int Cl' Ｇ１０Ｋ１５／００～１５／０６，Ｇ１０Ｌ１９／００～１９／１４，Ｈ０４Ｌ９／００～９／３８，
Ｇ０９Ｃ１／００～５／００，Ｇ０６Ｆ１２／００，Ｇ０６Ｆ１２／１４，Ｈ０４Ｍ１１／００～１１／１０

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２６～１９９５年
日本国公開実用新案公報　１９７１～２０００年
日本国登録実用新案公報　１９９４～２０００年
日本国実用新案登録公報　１９９６～２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）
ＷＰＩ（ＤＩＡＬＯＧ）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＥＰ，８１７１８５，Ａ２(Kabushiki kaisha TOSHIBA) 7.1月.1998(07.01.98)，全文全図， &JP,10-106148,A &JP,3093678,B2 &TW,340920,A &KR,98086354,A &CN,1183685,A	1
Y		2-22
X	ＪＰ，９－３２６１６６，Ａ(三菱電機株式会社) 16.12月.1997(16.12.97)，全文全図，（ファミリーなし）	1
Y		2-22

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１０．１１．００	21.11.0[illegible]

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	松尾　淳一　印　　５Ｃ　８８４２ 電話番号　０３－３５８１－１１０１　内線　３５４０

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，１０－４０１７２，Ａ(株式会社東芝) 13.2月.1998(13.2.98)，全文全図，（ファミリーなし）	2-22
Ｙ	日経エレクトロニクス，No.739，「小型メモリ・カードで音楽著作権を守る」，22.3月.1999(22.03.99)，p.49-53	2-22
Ｙ	日経エレクトロニクス，No.728，「米周辺機器メーカ大手が，ＭＰ３携帯型プレーヤ発売　著作権対策は付加せず」， 19.10月.1998(19.10.98)，p.31-32	2-22
Ａ	日経エレクトロニクス，No.731，「汚れたイメージ払拭ねらうＭＰ３業界 音楽配信の会議 Webnoise から」， 30.11月.1998(30.11.98)，p.29-30	1-22

IST

特 許 協 力 条 約

PCT

国際予備審査報告

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　９００３９２	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５８３２	国際出願日（日.月.年）　２９．０８．００	優先日（日.月.年）　３０．０８．９９
国際特許分類（ＩＰＣ）　Int Cl' G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10, G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08, G10L19/00		
出願人（氏名又は名称）　富士通株式会社		

１．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．　この国際予備審査報告は、この表紙を含めて全部で　4　ページからなる。

[X] この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で　１９　ページである。

３．　この国際予備審査報告は、次の内容を含む。

- I [X] 国際予備審査報告の基礎
- II [ ] 優先権
- III [ ] 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- IV [ ] 発明の単一性の欠如
- V [X] ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- VI [ ] ある種の引用文献
- VII [X] 国際出願の不備
- VIII [ ] 国際出願に対する意見

国際予備審査の請求書を受理した日　２６．０３．０１	国際予備審査報告を作成した日　１７．０９．０１
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｃ　９３７９ 樫本　剛 電話番号　０３－３５８１－１１０１　内線　３５４１

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５８３２

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。
ＰＣＴ規則70.16, 70.17）

☐ 出願時の国際出願書類

☒ 明細書　第 4 - 35 ページ、　出願時に提出されたもの
明細書　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書　第 1 - 3, 3/1- 3/4 ページ、　２０．０６．０１ 付の書簡と共に提出されたもの

☒ 請求の範囲　第 　　項、　出願時に提出されたもの
請求の範囲　第 　　項、　ＰＣＴ１９条の規定に基づき補正されたもの
請求の範囲　第 　　項、　国際予備審査の請求書と共に提出されたもの
請求の範囲　第 1 - 41 項、　２０．０６．０１ 付の書簡と共に提出されたもの

☒ 図面　第 1 - 22 ~~ページ~~図、　出願時に提出されたもの
図面　第 　　ページ／図、　国際予備審査の請求書と共に提出されたもの
図面　第 　　ページ／図、　　付の書簡と共に提出されたもの

☐ 明細書の配列表の部分　第 　　ページ、　出願時に提出されたもの
明細書の配列表の部分　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分　第 　　ページ、　　付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である 　　語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。
☐ 明細書　第 　　ページ
☐ 請求の範囲　第 　　項
☐ 図面　図面の第 　　ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５８３２

Ⅴ．　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）	請求の範囲	１－４１	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	１－４１	有
	請求の範囲		無
産業上の利用可能性（ＩＡ）	請求の範囲	１－４１	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

請求項１－５

文献１：ＥＰ　８１７１８５　Ａ２(Kabushiki kaisha TOSHIBA) 7.1月.1998 (07.01.98)

および

文献２：日経エレクトロニクス，No.739，「小型メモリ・カードで音楽著作権を守る」，22.3月.1999(22.03.99)，p.49-53

には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、データ再生部に固有な鍵にて復号可能な暗号を施された暗号化コンテンツキーをデータ格納部に格納する技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

請求項６－１１

文献１および文献２には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、コンテンツキーの取得のためのアクセスごとに異なるセッションキーをデータ再生部に固有な鍵により復号可能な暗号化を施して、データ再生部に供給するデータ格納部の技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

請求項１２－２２，３１－４１

文献１および文献２には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、コンテンツデータの取得のためのアクセスごとに異なるセッションキーをデータ再生部に固有な鍵により復号可能な暗号化を施して、データ再生部に供給するデータ格納部の技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

請求項２３－３０

文献１および文献２には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、データ再生部に固有な鍵および別のセッションキーにより暗号化を施されたセッションキーを用いたデータ再生モジュールの技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

Ⅶ.　国際出願の不備

この国際出願の形式又は内容について、次の不備を発見した。

明細書第３６頁第１２行に記載された「セッションキー発生部」には「１５２０」の記号が付されているが、第４図の符号「１５２０」の部分は「セッションキー発生部」ではなく「復号処理部」である。したがって、記号が国際出願の全体を通じて一貫して使用されていない。

また、明細書第３６頁第１４～１５行に記載された「第１の暗号化処理部」には「１５４０」の記号が付されているが、第４図の符号「１５４０」の部分は「第１の暗号化処理部」ではなく「Ｋｐ保持部」である。したがって、記号が国際出願の全体を通じて一貫して使用されていない。

明細書

データ再生装置およびデータ再生モジュール

技術分野

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽データや画像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権データの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモリカードのように電気的にデー

タの書込および消去が可能な媒体が用いられることになる。

さらに、配信データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティ対策を施す必要がある。

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができるとすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来たすことになる。

発明の開示

本発明の目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

係る目的を達成するために本願発明に係るデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ再生部と、データ格納部とを備える。

データ再生部は、暗号化コンテンツデータを再生する。データ格納部は、暗号化コンテンツデータと暗号化コンテンツデータを復号するためのコンテンツキーをデータ再生部に固有な第１の復号鍵にて復号可能な暗号を施された暗号化コンテンツキーとを格納し、かつデータ再生部に出力する。

データ再生部は、セッションキー発生部と、第１の暗号化処理部と、第１の復号処理部と、第１の鍵保持部と、第２の復号処理部と、第３の復号処理部とを含

む。

セッションキー発生部は、データ格納部に対してコンテンツキーの取得のためにアクセスするごとに更新されるセッションキーを生成する。第１の暗号化処理部は、セッションキーをデータ格納部にて復号可能で、かつデータ格納部に固有な公開暗号鍵で暗号化してデータ格納部に与える。第１の復号処理部は、セッションキーで暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、セッションキーを用いて復号する。

第１の鍵保持部は、第１の復号鍵を予め保持する。第２の復号処理部は、第１の鍵保持部に保持される第１の復号鍵を用いて第１の復号処理部からの出力に対して復号処理を行なうことで、コンテンツキーを抽出する。第３の復号処理部は、データ格納部から読出された暗号化コンテンツデータを受けて、第２の復号処理部にて抽出されたコンテンツキーを用いて復号してコンテンツデータを抽出する。

この発明の他の局面に従うと、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ再生部と、データ格納部とを備える。

データ再生部は、暗号化コンテンツデータを暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号してコンテンツデータを再生する。データ格納部は、暗号化コンテンツデータおよびコンテンツキーを格納し、コンテンツキーの取得のためにアクセスされるごとに異なる第１のセッションキーをデータ再生部に固有な固有復号鍵により復号可能な暗号化を施して、データ再生部に供給する。

データ再生部は、第１の鍵保持部と、第１の復号処理部と、第１のセッションキー発生部と、第１の暗号処理部と、第２の復号処理部と、第３の復号処理部を含む。

第１の鍵保持部は、固有復号鍵を予め保持する。第１の復号処理部は、第１の鍵保持部からの出力である固有復号鍵を用いて復号処理を行なう。第１のセッションキー発生部は、データ格納部に対してコンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成する。第１の暗号処理部は、データ格納部から供給された固有復号鍵にて復号可能な暗号化を施された第１の

セッションキーを第１の復号処理部にて復号し、復号された第１のセッションキーにより、第２のセッションキーを暗号化してデータ格納部に与える。第２の復号処理部は、固有復号鍵にて復号可能な暗号化を施され、かつ、第２のセッションキーで暗号化された上でデータ格納部から供給されたコンテンツキーを、第２のセッションキーについて復号する。第１の復号処理部は、固有復号鍵を用いて第２の復号処理部からの出力に対してさらに復号処理を行なうことで、コンテンツキーを抽出する。第３の復号処理部は、データ格納部から供給された暗号化コンテンツデータを受けて、第１の復号処理部により抽出されたコンテンツキーにより復号して、コンテンツデータを抽出する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ再生部と、データ格納部とを備える。

データ再生部は、暗号化コンテンツデータを暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号して、コンテンツデータを再生する。データ格納部は、暗号化コンテンツデータおよびコンテンツキーを格納し、かつ、暗号化コンテンツデータの取得のためのアクセスされるごとに異なる第１のセッションキーをデータ再生部に固有な固有復号鍵により復号可能な暗号化を施してデータ再生部に供給する。

データ再生部は、鍵保持部と、第１の復号処理部と、セッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第３の復号処理部とを備える。

鍵保持部は、固有復号鍵を予め保持する。第１の復号処理部は、データ格納部から供給された固有復号鍵にて復号可能な暗号化を施された第１のセッションキーを、固有復号鍵にて復号して抽出する。セッションキー発生部は、データ格納部に対してコンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成する。第１の暗号化処理部は、第２のセッションキーを第１のセッションキーで暗号化してデータ格納部に与える。第２の復号処理部は、第２のセッションキーで暗号化されてデータ格納部から供給されたコンテンツキーを、第２のセッションキーについて復号する。第３の復号処理部は、データ格納部から供給された暗号化コンテンツデータを受けて、第２の復号処理部の出力

に基づいて復号してコンテンツデータを抽出する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータを復号してコンテンツデータを再生するためのデータ再生装置に搭載するデータ再生モジュールであって、第１の鍵保持部と、第１の復号処理部と、セッションキー発生部と、暗号化処理部と、第２の復号処理部と、第３の復号処理部とを備える。

第１の鍵保持部は、データ再生モジュールに固有な第１の復号鍵を予め保持する。第１の復号処理部は、暗号化コンテンツデータを復号するための復号鍵であるコンテンツキーの取得のためのアクセスごとに第２の復号鍵により復号可能な暗号化処理を施されてデータ再生モジュールの外部から供給される第１のセッションキーを、第１の復号鍵にて復号して抽出する。セッションキー発生部は、データ再生モジュールの外部に対してコンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成する。暗号化処理部は、第２のセッションキーを第１のセッションキーを用いて暗号化してデータ再生モジュールの外部に与える。第２の復号処理部は、第２のセッションキーで暗号化されてデータ再生モジュールの外部から供給されるコンテンツキーを、第２のセッションキーを用いて復号する。第３の復号処理部は、データ再生モジュールの外部から供給される暗号化コンテンツデータを受けて、第２の復号処理部の出力に基づいて復号してコンテンツデータを抽出する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータおよび暗号化コンテンツデータを復号してコンテンツデータを得るための復号鍵であるコンテンツキーを格納し、かつ暗号化コンテンツデータの取得のためにアクセスされるごとに異なる第１のセッションキーをデータ再生装置に固有な固有復号鍵により復号可能な暗号化を施してデータ再生装置に供給するデータ記録部を装着して、データ記録装置に格納された暗号化コンテンツデータを、データ記録装置に格納された暗号化コンテンツキーを用いて再生するためのデータ再生装置であって、第１のインターフェイスと、鍵保持部と、第１の復号処理部と、セッションキー発生部と、暗号化処理部と、第２の復号処理部と、第３の復号処理部とを備える。

第１のインターフェイスは、データ記録装置を装着し、かつ、データ記録装置との間でデータの授受を行なう。鍵保持部は、データ再生装置に固有な固有鍵を

予め保持する。第１の復号処理部は、コンテンツキーの取得のためのアクセスごとに更新され、かつデータ再生装置に固有な固有復号鍵により復号可能な暗号化を施されてデータ記録装置から供給される第１のセッションキーを、固有復号鍵にて復号して抽出する。セッションキー発生部は、データ記録装置に対する暗号化コンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成する。暗号化処理部は、第２のセッションキーを第１のセッションキーを用いて暗号化してデータ記録装置に与える。第２の復号処理部は、第２のセッションキーで暗号化されてデータ記録装置から供給されるコンテンツキーを、第２のセッションキーを用いて復号する。第３の復号処理部は、データ記録装置から読出された暗号化コンテンツデータを受けて、第２の復号処理部の出力に基づいて復号してコンテンツデータを抽出する。

したがって、本願発明にかかるデータ再生装置によれば、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

図面の簡単な説明

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

図３は、携帯電話機１００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図４は、本発明の実施例２の携帯電話機２００の構成を説明するための概略ブロック図である。

図５は、図４に示した携帯電話機２００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図６は、図４に示したメモリカード１２０の構成を説明するための概略ブロッ

ク図である。

図７は、携帯電話機２００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図８は、本発明の実施例３の携帯電話機３００の構成を説明するための概略ブロック図である。

図９は、図８に示した携帯電話機３００において使用される通信のためのキー

請求の範囲

1．（補正後）暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（２００）であって、

前記暗号化コンテンツデータを再生するためのデータ再生部（１５００）と、

前記暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのコンテンツキーを前記データ再生部に固有な第１の復号鍵にて復号可能な暗号を施された暗号化コンテンツキーとを格納し、かつ前記データ再生部に出力するためのデータ格納部（１２０）とを備え、

前記データ再生部は、

前記データ格納部に対して前記コンテンツキーの取得のためにアクセスするごとに更新されるセッションキーを生成するセッションキー発生部（１５２０）と、

前記セッションキーを前記データ格納部にて復号可能で、かつ前記データ格納部に固有な公開暗号鍵で暗号化して前記データ格納部に与えるための第１の暗号化処理部（１５４０）と、

前記セッションキーで暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記セッションキーを用いて復号する第１の復号処理部（１５０６）と、

前記第１の復号鍵を予め保持する第１の鍵保持部（１５４０）と、

前記第１の鍵保持部に保持される前記第１の復号鍵を用いて前記第１の復号処理部からの出力に対して復号処理を行なうことで、前記コンテンツキーを抽出する第２の復号処理部（１５３０）と、

前記データ格納部から読出された前記暗号化コンテンツデータを受けて、前記第２の復号処理部にて抽出されたコンテンツキーを用いて復号してコンテンツデータを抽出するための第３の復号処理部（１５２０）とを含む、データ再生装置。

2．（補正後）前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音

楽再生部（１５０８）と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（１５１２）とをさらに含む、請求項１に記載のデータ再生装置。

３．（補正後）前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項１に記載のデータ再生装置。

４．（補正後）前記データ格納部（１２０）は、

前記データ格納部に与えられるデータを保持するための記録部（１４１２）と、

前記データ格納部に固有な前記公開暗号鍵を保持し、前記データ再生部へ供給可能な第２の鍵保持部（１４０１）と、

前記公開暗号鍵により暗号化されたデータを復号するための第２復号鍵を保持する第３の鍵保持部（１４０２）と、

前記第２の復号鍵を用いて、前記データ再生部から前記公開暗号鍵により暗号化されて伝達された前記第１のセッションキーを復号するための第４の復号処理部（１４０４）と、

前記第４の復号処理部で抽出された前記第１のセッションキーにより、前記記録部に格納された暗号化コンテンツキーを暗号化して出力するための第２の暗号化処理部（１４０６）とを備える、請求項１に記載のデータ再生装置。

５．（補正後）前記データ格納部は、前記データ再生部に対して着脱可能である、請求項１に記載のデータ再生装置。

６．（補正後）暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（３００、４００）であって、

前記暗号化コンテンツデータを前記暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号してコンテンツデータを再生するためのデータ再生部（１５００）と、

前記暗号化コンテンツデータおよび前記コンテンツキーを格納し、前記コンテンツキーの取得のためにアクセスされるごとに異なる第１のセッションキーを前記データ再生部に固有な固有復号鍵により復号可能な暗号化を施して、前記データ再生部に供給するデータ格納部（１３０，１４０）とを備え、

前記データ再生部は、

前記固有復号鍵を予め保持する第１の鍵保持部（１５４０）と、

前記第１の鍵保持部からの出力である前記固有復号鍵を用いて復号処理を行なう第１の復号処理部（１５３０）と、

前記データ格納部に対して前記コンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成する第１のセッションキー発生部（１５２２）と、

前記データ格納部から供給された前記固有復号鍵にて復号可能な暗号化を施された前記第１のセッションキーを前記第１の復号処理部にて復号し、復号された前記第１のセッションキーにより、前記第２のセッションキーを暗号化して前記データ格納部に与えるための第１の暗号処理部（１５５４）と、

前記固有復号鍵にて復号可能な暗号化を施され、かつ、前記第２のセッションキーで暗号化された上で前記データ格納部から供給された前記コンテンツキーを、前記第２のセッションキーについて復号する第２の復号処理部（１５５６）とを含み、

前記第１の復号処理部は、前記固有復号鍵を用いて前記第２の復号処理部からの出力に対してさらに復号処理を行なうことで、前記コンテンツキーを抽出し、

前記データ格納部から供給された前記暗号化コンテンツデータを受けて、前記第１の復号処理部により抽出されたコンテンツキーにより復号して、コンテンツデータを抽出するための第３の復号処理部（１５２０）をさらに含む、データ再生装置。

７．（補正後）前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項６に記載のデータ再生装置。

８．（補正後）前記データ再生部は、

少なくとも前記第１の鍵保持部と、前記第１の復号処理部と、前記第２の復号

処理部と、前記第３の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられる、請求項７に記載のデータ再生装置。

９．（補正後）前記データ格納部（１３０，１４０）は、

前記データ格納部に与えられるデータを格納するための記録部（１４１２）と、

前記第１のセッションキーを発生する第２のセッションキー発生部（１４５０）と、

前記データ再生部に固有でかつ前記固有復号鍵にて復号可能な暗号化を施すための公開暗号鍵により、暗号化処理を行なう第２の暗号化処理部（１４５２）と、

前記第１のセッションキーを用いて、前記データ再生部から前記第１のセッションキーにて暗号化されて伝達された前記第２のセッションキーを復号するための第４の復号処理部（１４５４）と、

前記第４の復号処理部にて抽出された前記第１のセッションキーにより、暗号化処理を行ない出力するための第３の暗号化処理部（１４５６）とを備え、

前記記録部に格納された前記コンテンツキーを前記第２の暗号化処理部にて暗号化し、さらに前記第３の暗号化処理部にて暗号化して、前記データ再生部に供給する、請求項６に記載のデータ再生装置。

１０．（補正後）前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項６に記載のデータ再生装置。

１１．（補正後）前記データ再生装置は、

前記データ再生部に固有な認証データとともに前記公開暗号鍵を、前記データ格納部にて認証鍵により復号可能な暗号化を施して保持し、前記データ格納部に供給する認証データ保持部（１５６０）をさらに備え、

前記データ格納部（１４０）は、

前記認証鍵により暗号化されて前記データ再生部から与えられる前記認証データと前記公開暗号鍵を復号して抽出するための第５の復号処理部（１４６０）と、

前記第５の復号処理部により抽出された前記認証データに基づいて前記認証データを出力したデータ再生部に対して前記コンテンツキーを出力するか否かを判断する認証処理を行なう制御手段（１４２０）とを含む、請求項９に記載のデータ再生装置。

１２．（補正後）暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（５００，６００）であって、

前記暗号化コンテンツデータを前記暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号して、コンテンツデータを再生するためのデータ再生部と、

前記暗号化コンテンツデータおよび前記コンテンツキーを格納し、かつ、前記暗号化コンテンツデータの取得のためのアクセスされるごとに異なる第１のセッションキーを前記データ再生部に固有な固有復号鍵により復号可能な暗号化を施して前記データ再生部に供給するデータ格納部（１５０，１６０）とを備え、

前記データ再生部は、

前記固有復号鍵を予め保持する鍵保持部（１５４０）と、

前記データ格納部から供給された前記固有復号鍵にて復号可能な暗号化を施された前記第１のセッションキーを、前記固有復号鍵にて復号して抽出する第１の復号処理部（１５３０）と、

前記データ格納部に対して前記コンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成するセッションキー発生部（１５５２）と、

前記第２のセッションキーを前記第１のセッションキーで暗号化して前記データ格納部に与えるための第１の暗号化処理部（１５５４）と、

前記第２のセッションキーで暗号化されて前記データ格納部から供給された前記コンテンツキーを、前記第２のセッションキーについて復号する第２の復号処理部（１５５６）と、

前記データ格納部から供給された前記暗号化コンテンツデータを受けて、前記第２の復号処理部の出力に基づいて復号してコンテンツデータを抽出するための第３の復号処理部（１５２０）とを備える、データ再生装置。

１３．（補正後）前記データ再生部に固有でかつ前記固有復号鍵にて復号可能な暗号化を施すための暗号鍵である公開暗号鍵と前記データ再生部に固有な認証データとを認証鍵により復号可能な暗号化を施した上で保持し、前記データ格納部に対して出力可能な認証データ保持部（１５６０）をさらに備える、請求項１２

記載のデータ再生装置。

１４．（補正後）前記データ格納部は前記データ再生装置から着脱可能である、請求項１３記載のデータ再生装置。

１５．（補正後）前記コンテンツキーは、

前記データ再生装置に予め定められた第２の復号鍵にて復号可能な暗号化を施されて、前記記録部に格納され、

前記データ再生部は、予め定められた第２の復号鍵にて復号するための第５の復号処理部（１５７２）をさらに備え、

前記第５の復号処理部は、

前記第２の復号鍵で復号可能な暗号化を施されて、さらに、前記第２のセッションキーで暗号化された上で前記データ格納部から供給された前記コンテンツキーを、前記第２の復号処理部が前記第２のセッションキーについて復号した結果を入力として受け、前記第２の復号鍵にて復号し、前記第３の復号処理部に与える、請求項１２に記載のデータ再生装置。

１６．（補正後）前記データ格納部は、前記データ再生装置に対して着脱可能である、請求項１２に記載のデータ再生装置。

１７．（補正後）前記データ再生装置は、さらに、携帯電話網に接続するインターフェイスを備える、請求項１２に記載のデータ再生装置。

１８．（補正後）前記データ再生装置は、さらに、前記インターフェイスを介して通話を行なうための通話処理部を備える、請求項１７に記載のデータ再生装置。

１９．（補正後）前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項１２に記載のデータ再生装置。

２０．（補正後）前記データ再生部は、

少なくとも前記鍵保持部と、前記第１の復号処理部と、前記第２の復号処理部と、前記第３の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている、請求項１２に記載のデータ再生装置。

２１．（補正後）前記データ格納部（１５０，１６０）は、

前記データ格納部に与えられるデータを格納するための記録部（１４１２）と、

前記第１のセッションキーを発生する第２のセッションキー発生部（１４５

０）と、

前記コンテンツデータ再生部に固有でかつ前記固有復号鍵にて復号可能な暗号化を施すための公開暗号鍵により、前記第２のセッションキー発生部にて生成した前記第１のセッションキーを暗号化する第２の暗号化処理部（１４５２）と、

前記第１のセッションキーを用いて、前記データ再生部から前記第１のセッションキーにて暗号化されて伝達された前記第２のセッションキーを復号するための第４の復号処理部（１４５４）と、

前記第４の復号処理部にて抽出された前記第２のセッションキーにより、暗号化処理を行ない出力するための第３の暗号化処理部（１４５６）とを備え、

前記記録部に格納された前記コンテンツキーを前記第３の暗号化処理部にて暗号化して、前記データ再生部に供給する、請求項１２に記載のデータ再生装置。

２２．（補正後）前記データ格納部（１５０，１６０）は、

前記データ格納部に与えられるデータを格納するための記録部（１４１２）と、

前記認証鍵により復号可能な暗号化を施された前記公開暗号鍵と前記認証データを前記認証鍵にて復号して前記公開鍵と前記認証データを抽出するための第４の復号処理部（１４６０）と、

前記第４の復号処理部にて抽出された前記認証データに基づいて前記認証データを出力したデータ再生部に対して前記コンテンツキーを出力するか否か判断する認証処理の制御を行なう制御部（１４２０）と、

前記第１のセッションキーを発生する第２のセッションキー発生部（１４５０）と、

前記第４の復号処理部にて抽出された前記公開暗号鍵により、前記第２のセッションキー発生部にて生成した前記第１のセッションキーを暗号化する第２の暗号化処理部（１４５２）と、

前記第１のセッションキーを用いて、前記データ再生部から前記第１のセッションキーにて暗号化されて伝達された前記第２のセッションキーを復号するための第４の復号処理部（１４５４）と、

前記第４の復号処理部にて抽出された前記第２のセッションキーにより、暗号化処理を行ない出力するための第３の暗号化処理部（１４５６）とを備え、

前記記録部に格納された前記コンテンツキーを前記第３の暗号化処理部にて暗号化して、前記データ再生部に供給する、請求項１３に記載のデータ再生装置。

２３．（追加）暗号化コンテンツデータを復号してコンテンツデータを再生するためのデータ再生装置に搭載するデータ再生モジュール（１５００）であって、

前記データ再生モジュールに固有な第１の復号鍵を予め保持する第１の鍵保持部（１５４０）と、

前記暗号化コンテンツデータを復号するための復号鍵であるコンテンツキーの取得のためのアクセスごとに前記第２の復号鍵により復号可能な暗号化処理を施されて前記データ再生モジュールの外部から供給される第１のセッションキーを、前記第１の復号鍵にて復号して抽出する第１の復号処理部（１５３０）と、

前記データ再生モジュールの外部に対して前記コンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成するセッションキー発生部（１５５２）と、

前記第２のセッションキーを前記第１のセッションキーを用いて暗号化して前記データ再生モジュールの外部に与える暗号化処理部（１５５４）と、

前記第２のセッションキーで暗号化されて前記データ再生モジュールの外部から供給される前記コンテンツキーを、前記第２のセッションキーを用いて復号する第２の復号処理部（１５５６）と、

前記データ再生モジュールの外部から供給される前記暗号化コンテンツデータを受けて、前記第２の復号処理部の出力に基づいて復号してコンテンツデータを抽出するための第３の復号処理部（１５２０）とを備える、データ再生モジュール。

２４．（追加）前記データ再生モジュールに固有でかつ前記第１の復号鍵にて復号可能な暗号鍵である公開暗号鍵と前記データ再生モジュールに固有な認証データとを前記データ再生モジュールの外部にて認証鍵により復号可能な暗号化を施して保持し、前記データ再生モジュールの外部に対して出力可能な認証データ保持部（１５６０）をさらに備える、請求項２３に記載のデータ再生モジュール。

２５．（追加）前記コンテンツキーは、前記第２のセッションキーで暗号化され前記データ再生モジュールの外部から入力され、前記第２の復号処理部（１５５

6）は、復号結果を前記暗号化コンテンツデータを復号するためのコンテンツキーとして前記第３の復号処理部（１５２０）に与える、請求項２３に記載のデータ再生モジュール。

２６．（追加）前記コンテンツキーは、前記第１の復号鍵にて復号可能な暗号化を施され、かつ前記第２のセッションキーで暗号化されて前記データ再生モジュールの外部から入力され、

前記第１の復号処理部は、さらに、前記第２の復号処理部（１５５６）の出力である前記第１の復号鍵にて復号可能な暗号化されたコンテンツキーを、前記第１の復号鍵を用いて復号し前記コンテンツキーを抽出して、前記第３の復号処理部（１５２０）に与える、請求項２３に記載のデータ再生モジュール。

２７．（追加）前記コンテンツキーは、前記第２の復号鍵にて復号可能な暗号化を施されかつ前記第２のセッションキーにて暗号化されて前記データ再生モジュールの外部から入力され、

前記データ再生モジュールは、

前記第２の復号鍵を予め保持する第２の鍵保持部（１５７０）と、

前記第２の復号処理部（１５５６）から出力される前記第２の復号鍵にて復号可能な暗号化を施された前記コンテンツキーを前記第２の復号鍵を用いて復号し、前記コンテンツキーを抽出して、前記第３の復号処理部（１５２０）に与える第４の復号処理部（１５７２）とをさらに備える、請求項２３に記載のデータ再生モジュール。

２８．（追加）前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化データであって、

前記データ再生モジュールは、

前記符号化データから前記符号化方式に基づいてデータを再生する再生部（１８０８）をさらに含む、請求項２３に記載のデータ再生モジュール。

２９．（追加）前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生モジュールは、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音

楽再生部（１８０８）と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（１５１２）とをさらに含む、請求項２３に記載のデータ再生モジュール。

３０．（追加）前記データ再生モジュールは、タンパーデジスタンスモジュールである、請求項２３記載のデータ再生モジュール。

３１．（追加）暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号してコンテンツデータを得るための復号鍵であるコンテンツキーを格納し、かつ前記暗号化コンテンツデータの取得のためにアクセスされるごとに異なる第１のセッションキーをデータ再生装置に固有な固有復号鍵により復号可能な暗号化を施して前記データ再生装置に供給するデータ記録装置（１３０，１４０，１５０，１６０）を装着して、前記データ記録装置に格納された前記暗号化コンテンツデータを、前記データ記録装置に格納されたコンテンツキーを用いて再生するためのデータ再生装置（３００，４００，５００，６００）であって、

前記データ記録装置を装着し、かつ、前記データ記録装置との間でデータの授受を行なうための第１のインターフェイス（１２００）と、

前記データ再生装置に固有な固有鍵を予め保持する鍵保持部（１５４０）と、

前記コンテンツキーの取得のためのアクセスごとに更新され、かつ前記データ再生装置に固有な前記固有復号鍵により復号可能な暗号化を施されて前記データ記録装置から供給される第１のセッションキーを、前記固有復号鍵にて復号して抽出する第１の復号処理部（１５３０）と、

前記データ記録装置に対する前記暗号化コンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成するセッションキー発生部（１５５２）と、

前記第２のセッションキーを前記第１のセッションキーを用いて暗号化して前記データ記録装置に与えるための暗号化処理部（１５５４）と、

前記第２のセッションキーで暗号化されて前記データ記録装置から供給される前記コンテンツキーを、前記第２のセッションキーを用いて復号する第２の復号処理部（１５５６）と、

前記データ記録装置から読出された前記暗号化コンテンツデータを受けて、前

記第２の復号処理部の出力に基づいて復号してコンテンツデータを抽出するための第３の復号処理部（１５２０）とを備える、データ再生装置。

３２．（追加）前記データ再生装置に固有でかつ、前記第１の復号鍵にて復号可能な暗号鍵である公開暗号鍵と前記データ再生装置に固有な認証データを前記データ記録装置にて認証鍵による復号可能な暗号化を施して保持し、前記データ記録装置に対して出力する認証データ保持部（１５６０）をさらに備える、請求項３１に記載のデータ再生装置。

３３．（追加）前記コンテンツキーは、前記第２のセッションキーで暗号化されて前記データ記録装置（１５０）から供給され、前記第２の復号処理部（１５５６）は、復号結果を前記暗号化コンテンツデータを復号するためのコンテンツキーとして前記第３の復号処理部（１５２０）に与える、請求項３１記載のデータ再生装置。

３４．（追加）前記コンテンツキーは、前記第１の復号鍵にて復号可能な暗号化を施され、かつ前記第２のセッションキーで暗号化されて前記データ記録装置（１３０，１４０）から供給され、

前記第１の復号処理部は、さらに、前記第２の復号処理部（１５５６）の出力である前記第１の復号鍵にて復号可能な暗号化されたコンテンツキーを、前記第１の復号鍵を用いて復号し前記コンテンツキーを抽出して、前記第３の復号処理部（１５２０）に与える、請求項３１記載のデータ再生装置。

３５．（追加）前記コンテンツキーは、前記第２の復号鍵にて復号可能な暗号化を施され、かつ前記第２のセッションキーで暗号化されて前記データ記録装置（１６０）から供給され、

前記データ再生装置は、

前記第２の復号鍵を予め保持する第２の鍵保持部（１５７０）と、

前記第２の復号処理部（１５５６）から出力される前記第２の復号鍵にて復号可能な暗号化を施された前記コンテンツキーを前記第２の復号鍵を用いて復号し、前記コンテンツキーを抽出して、前記第３の復号処理部（１５２０）に与える第４の復号処理部（１５７２）とをさらに備える、請求項３１記載のデータ再生装置。

３６．（追加）前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化データであって、

前記データ再生装置は、

前記符号化データから前記符号化方式に基づいてデータを再生する再生部（１８０８）をさらに含む、請求項３１記載のデータ再生装置。

３７．（追加）前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生装置は、前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部（１８０８）と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（１５１２）とをさらに含む、請求項３１記載のデータ再生装置。

３８．（追加）前記データ再生装置は、さらに、携帯電話網に接続する第２のインターフェイスを備える、請求項３１記載のデータ再生装置。

３９．（追加）前記データ再生装置は、さらに、前記第２のインターフェイスを介して通話を行なうための通話処理部を備える、請求項３８記載のデータ再生装置。

４０．（追加）前記データ再生装置は、

第三者には読出不可能なセキュリティ領域を備えて、

少なくとも前記第１の鍵保持部と、前記第１の復号処理部と、前記第２の復号処理部と、前記第３の復号処理部とが、前記セキュリティ領域に設けられている、請求項３１記載のデータ再生装置。

４１．（追加）前記データ再生装置は、

第三者に読出不可能なセキュリティ領域を備えて、

少なくとも前記第１の鍵保持部と、前記第２の鍵保持部と、前記第１の復号処理部と、前記第２の復号処理部と、前記第３の復号処理部と、前記第２の復号処理部とが、前記セキュリティ領域に設けられている、請求項３１記載のデータ再生装置。

(12)特許協力条約に基づいて公開された国[redacted]

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年3月8日 (08.03.2001)

PCT

(10) 国際公開番号
WO 01/16933 A1

(51) 国際特許分類[7]: G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H 1/00, H04M 3/42, 3/493, 11/08, G10L 19/00

(21) 国際出願番号: PCT/JP00/05832

(22) 国際出願日: 2000年8月29日 (29.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/243583 1999年8月30日 (30.08.1999) JP
特願平11/343707 1999年12月2日 (02.12.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 畑中正行 (HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KAMADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]. 古田茂樹 (FURUTA, Shigeki) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

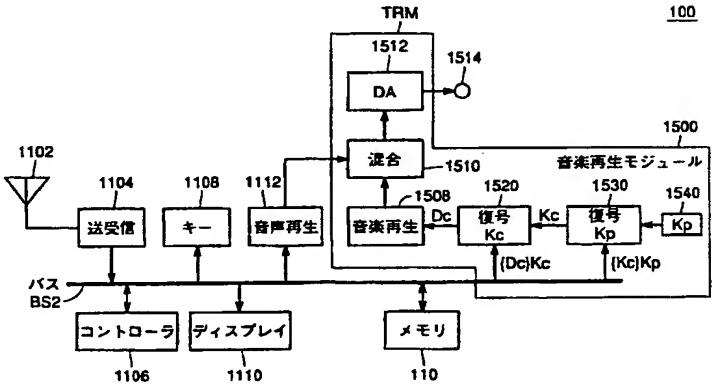
(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[続葉有]

(54) Title: DEVICE FOR DATA REPRODUCTION

(54) 発明の名称: データ再生装置



110...MUSIC PLAYBACK
1104...TRANSMISSION/RECEPTION
1106...CONTROLLER
1108...KEY
1110...DISPLAY
1112...AUDIO PLAYBACK
1500...MUSIC PLAYBACK MODULE
1508...MUSIC PLAYBACK
1510...MIX
1520...DECRYPT Kc
1530...DECRYPT Kp
BS2...BUS

(57) Abstract: A cellular phone (100) stores distributed encrypted content data and encrypted content key in memory (110). The encrypted content key data read from the memory (110) is decrypted by decryption means (1530) using key data (kp) held by a Kp holder (1540), and then input to music playback module (1500). The encrypted content data read from the memory (110) is decrypted by decryption means (1520) using a content key (Kc) extracted by decryption means (1530), and content data (Dc) is reproduced.

[続葉有]

WO 01/16933 A1

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

携帯電話機（１００）は、配信された暗号化コンテンツデータおよび暗号化コンテンツキーをメモリ（１１０）に格納する。メモリ（１１０）から読み出された暗号化コンテンツキーデータは、Ｋｐ保持部（１５４０）の保持するキーデータＫｐにより復号処理部（１５３０）により復号されて、音楽再生モジュール（１５００）に取り込まれる。復号処理部（１５２０）は、メモリ（１１０）から読み出した暗号化コンテンツデータを、復号処理部（１５３０）により抽出されたコンテンツキーＫｃにより復号して、コンテンツデータＤｃを再生する。

明細書

データ再生装置

技術分野

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽データや画像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権データの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモリカードのように電気的にデー

タの書込および消去が可能な媒体が用いられることになる。

さらに、配信データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティ対策を施す必要がある。

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができるとすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来たすことになる。

発明の開示

本発明の目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

係る目的を達成するために本願発明に係るデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ格納部と、データ再生部とを備える。

データ格納部は、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納する。

データ再生部は、データ格納部からの出力を受けて、暗号化コンテンツデータを再生する。データ再生部は、第１の鍵保持部と、第１の復号処理部と、第２の復号処理部とを含む。

第１の鍵保持部は、データ格納部から読み出された暗号化コンテンツキーを復

号するための第１の復号鍵を保持する。第１の復号処理部は、データ格納部からの暗号化コンテンツキーを基にして、第１の鍵保持部からの出力により復号処理を行なうことで、コンテンツキーを抽出する。第２の復号処理部は、データ格納部から読み出された暗号化コンテンツデータを受けて、第１の復号処理部の出力により復号してコンテンツデータを抽出する。

したがって、本願発明にかかるデータ再生装置によれば、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

図面の簡単な説明

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

図３は、携帯電話機１００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図４は、本発明の実施例２の携帯電話機２００の構成を説明するための概略ブロック図である。

図５は、図４に示した携帯電話機２００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図６は、図４に示したメモリカード１２０の構成を説明するための概略ブロック図である。

図７は、携帯電話機２００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図８は、本発明の実施例３の携帯電話機３００の構成を説明するための概略ブロック図である。

図９は、図８に示した携帯電話機３００において使用される通信のためのキー

データ（鍵データ）等の特性をまとめて説明するための図である。

図１０は、図８に示したメモリカード１３０の構成を説明するための概略ブロック図である。

図１１は、携帯電話機３００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図１２は、本発明の実施例４の携帯電話機４００の構成を説明するための概略ブロック図である。

図１３は、図１２に示した携帯電話機４００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図１４は、図１２に示したメモリカード１４０の構成を説明するための概略ブロック図である。

図１５は、メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１６は、本発明の実施例５の携帯電話機５００の構成を説明するための概略ブロック図である。

図１７は、図１６に示したメモリカード１５０の構成を説明するための概略ブロック図である。

図１８は、メモリカード１５０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１９は、本発明の実施例６の携帯電話機６００の構成を説明するための概略ブロック図である。

図２０は、図１９に示した携帯電話機６００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図２１は、図１９に示したメモリカード１６０の構成を説明するための概略ブロック図である。

図２２は、メモリカード１６０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

［実施例１］

［システムの全体構成］

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、暗号化された音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、暗号化された他の著作物情報データ、例えば画像データ等の著作物情報データを、復号して平文化して再生することが可能なものである。

なお、ここで携帯電話網としては、ＰＨＳ（Personal Handy Phone）などの簡易携帯電話網も含むものとする。

図１を参照して、著作権の存在する音楽データを管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア２０である携帯電話会社に、このような暗号化データを与える。

配信キャリア２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。配信サーバ１０は、配信リクエストがあると、要求された暗号化音楽情報を携帯電話会社２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１４０等を介してこのような再生された音楽データを聴取することが可能である。

以下では、このような配信サーバ１０と配信キャリア（携帯電話会社）２０とを併せて、音楽サーバ３０と総称することにする。

また、このような音楽サーバ３０から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

しかも、配信キャリア２０において、たとえば１曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料

金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

［配信サーバ１０の構成］

図１において配信サーバ１０は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したコンテンツデータやコンテンツキー等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、暗号化コンテンツデータを復号するためのコンテンツキーＫｃを公開暗号化鍵ＫＰｐにより暗号化するためのコンテンツキー暗号化処理部３１６と、配信情報データベース３０４および課金データベース３０２とデータバスＢＳ１を介してデータ授受を行ない、配信サーバ１０の動作を制御するためのコントローラ３１２と、通信網を介して、配信サーバ１０と配信キャリア２０との間でデータ授受を行なうための通信装置３５０とを備える。

すなわち、配信情報データベース３０４からは、コンテンツデータＤｃが復号鍵であるコンテンツキーＫｃにより復号可能な状態に暗号化された暗号化コンテンツデータ［Ｄｃ］Ｋｃと、コンテンツキーＫｃとが出力される。コントローラ３１２は、コンテンツキー暗号化処理部３１６を制御して、このコンテンツキーＫｃを公開暗号化鍵ＫＰｐにより暗号化した［Ｋｃ］Ｋｐを通信装置３５０を介して、配信キャリア２０に与える。

ここで、［Ｙ］Ｘという表記は、データＹを、キー（鍵）Ｘにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

［端末（携帯電話機）の構成］

図２は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するための

アンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、外部からの指示を携帯電話機１００に与えるためのタッチキーやダイヤルキーなどを含むキーボード１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを備える。

携帯電話機１００は、さらに、サーバ３０からの暗号化コンテンツデータ［Ｄｃ］Ｋｃおよび暗号化コンテンツキー［Ｋｃ］Ｋｐを格納するためのメモリ１１０と、音楽再生モジュール１５００とを備える。この音楽再生モジュール１５００は、公開暗号化鍵ＫＰｐに対応し、キーＫＰｐで暗号化されたデータを復号可能な秘密復号鍵Ｋｐを保持するＫｐ保持部１５４０と、音楽サーバ３０から伝送され公開暗号化鍵ＫＰｐにより暗号化コンテンツキー［Ｋｃ］Ｋｐをメモリ１１０から受けて復号するための復号処理部１５３０と、音楽サーバ３０から配信されメモリ１１０中に格納された暗号化コンテンツデータ［Ｄｃ］Ｋｃを、復号処理部１５３０で復号抽出されたコンテンツキーＫｃに基づいて復号するための復号処理部１５２０と、復号処理部１５２０からの復号されたコンテンツデータを受けて、コンテンツデータを符号化した符号化方式、例えば、ＭＰ３（MPEG1 Audio Layer III）、ＡＣ３等のデジタル圧縮符号化方式の再生手順に従って音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２とを含む。

携帯電話機１００は、さらに、デジタルアナログ変換部１５１２の出力を受けて、ヘッドホン１４０と接続するための接続端子１５１４とを含む。

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図２に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０および復号処理部１５２０を、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組み込む構成とすることが可能である。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機１００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図２において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

［再生処理］

図３は、携帯電話機１００内において、メモリ１１０に保持された暗号化コンテンツデータから、コンテンツデータを復号して、音楽として外部に出力するための再生処理を説明するフローチャートである。

図３を参照して、携帯電話のキーボード１１０８等からのユーザの指示により、再生リクエストがコントローラ１１０６に与えられる（ステップＳ１００）。

この再生リクエストに応じて、コントローラ１１０６は、メモリ１１０を制御して暗号化コンテンツキー［Ｋｃ］Ｋｐを読み出す（ステップＳ１０２）。

つづいて、復号処理部１５３０は、メモリ１１０から読み出された暗号化コンテンツキー［Ｋｃ］Ｋｐに対する復号処理を行なう（ステップＳ１０４）。

復号処理部１５３０においてコンテンツキーＫｃを復号抽出可能な場合は（ステップＳ１０６）、処理は次のステップに移行し、一方、復号不能と判断された場合は、処理は終了する（ステップＳ１１０）。

復号処理部１５３０においてコンテンツキーＫｃを復号抽出可能な場合は、コントローラ１１０８は、メモリ１１０を制御して、暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、復号処理部１５２０に与え、復号処理部１５２０は、復号鍵Ｋｃにより復号処理して、平文化したコンテンツデータＤｃを生成して音楽再生部１５０８に与える。音楽再生部１５０８においてコンテンツデータＤｃより再生された音楽信号は、混合部１５１０を経由して、デジタルアナログ変換器１５１２によりアナログ信号に変換されて接続端子１５１４から外部に出力される。

以上のような構成とすることで、再生装置である携帯電話機１００内のメモリ１１０には、暗号化コンテンツデータと暗号化コンテンツキーが保持されているのみであるため、外部からこのメモリ１１０内の記憶内容を仮に読み出したとしても、音楽を再生することはできない。

しかも、メモリ１１０から復号処理部１５２０および１５３０に与えられるデータも、このような暗号化されたデータであるため、データバスＢＳ２上の信号を外部から仮に検出したとしても、音楽を再生することはできない。

さらに、平文化された音楽データが伝達される部分は、上述のとおり、タンパーレジスタンスモジュールで構成されているので、この部分から音楽データを外部に読み出すこともできない構成となっている。

したがって、図２に示した携帯電話機１００の構成により、不正な手続きでコンテンツデータを複製して、再生あるいは配布を行なうことから保護することが可能となる。

［実施例２］

図４は、本発明の実施例２の携帯電話機２００の構成を説明するための概略ブロック図であり、実施例１の図２と対比される図である。

図２に示した携帯電話機１００の構成と、携帯電話機２００の構成が異なる点は、以下のとおりである。

まず、図４においては、携帯電話機２００には、携帯電話機２００により受信された暗号化コンテンツデータを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機２０

０中の音楽再生モジュール１５００に与えるための着脱可能なメモリカード１２０が装着される構成となっている。これに応じて、携帯電話機２００は、メモリカード１２０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００をさらに備えている。

さらに、携帯電話機２００の構成では、音楽再生モジュール１５００の構成も、携帯電話機１００の構成と異なる。

すなわち、携帯電話機２００の音楽再生モジュール１５００は、メモリカード１２０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するための後に説明するセッションキーＫｓを乱数等により発生するセッションキー発生部１５０２と、セッションキー発生部１５０２により生成されたセッションキーＫｓを暗号化して、データバスＢＳ２に与えるための暗号化処理部１５０４と、データバスＢＳ２によりメモリカード１２０から伝送され、公開暗号化鍵ＫＰｐおよびセッションキーＫｓにより暗号化コンテンツキーＫｃをセッションキーＫｓについて復号して出力する復号処理部１５０６と、公開暗号化鍵ＫＰｐに対応し、キーＫＰｐで暗号化されたデータを復号可能な秘密復号鍵Ｋｐを保持するＫｐ保持部１５４０と、復号処理部１５０６の出力を受けて、メモリカード１２０から伝送され公開暗号化鍵ＫＰｐにより暗号化コンテンツキー［Ｋｃ］Ｋｐを復号するための復号処理部１５３０と、サーバ３０から配信されメモリカード１２０中に格納された暗号化コンテンツデータ［Ｄｃ］Ｋｃを、復号処理部１５３０で復号抽出されたコンテンツキーＫｃに基づいて復号するための復号処理部１５２０と、復号処理部１５２０からの復号されたコンテンツデータＤｃを受けて、音楽サーバ３０から配信された音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２とを含む。

携帯電話機２００のその他の部分は、実施例１の携帯電話機１００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図４においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図４に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５０６、暗号化処理部１５０４およびＫｓ発生部１５０２を、ＴＲＭに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機２００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図４において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータついても、保護することが可能である。

［暗号／復号鍵の構成］

図５は、図４に示した携帯電話機２００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図４に示した構成において、メモリカード１２０内のデータ処理を管理するための鍵としては、メモリカードに固有な公開暗号化鍵ＫＰｍと、公開暗号化鍵ＫＰｍにより暗号化されたデータを復号するためのキーＫＰｍとは非対称な秘密復号鍵Ｋｍとがある。

ここで、キーＫＰｍとキーＫｍとが非対称とは、複数の公開暗号化鍵ＫＰｍにより暗号化されたデータが、キーＫＰｍとは異なりＫＰｍからは容易に類推できない復号鍵Ｋｍにより復号できることを意味する。

したがって、メモリカード１２０と携帯電話機２００とのセッションキーの授受にあたっては、後に説明するようにこれら暗号化鍵Ｋｍ、復号鍵ＫＰｍが用いられることになる。

さらに、メモリカード外でのデータの授受における秘密保持のための暗号化鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵をＫＰｐと、音楽再

生モジュール管理の鍵として、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、各通信ごとにＫｓ発生器１５０２において生成される共通鍵Ｋｓとが用いられる。

ここで、共通鍵Ｋｓは、たとえば、携帯電話機２００とメモリカード１２０との間のコンテンツデータの授受のためのアクセスが行なわれるごとにＫｓ発生器１５０２において発生する。

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ｋｓを「セッションキー」とも呼ぶことにする。

したがって、セッションキーＫｓは各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

さらに、メモリカード１２０に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、このコンテンツキーＫｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

著作権の存在するコンテンツデータＤｃは、上述のとおり、たとえば音楽データであり、このコンテンツデータをコンテンツキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

また、配信サーバ１０から携帯電話機２００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも公開暗号化鍵ＫＰｐにより暗号化されており、メモリカード１２０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｐとして格納されているものとする。

［メモリカードの構成］

図６は、図４に示したメモリカード１２０の構成を説明するための概略ブロック図である。

メモリカード１２０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、公開暗号化鍵ＫＰｍの値を保持し、データバスＢＳ３に公開暗号化鍵ＫＰｍを出力するためのＫＰｍ保持部１４０１と、カード１２０に対応する秘密復号鍵Ｋｍを保持するためのＫｍ保持部１４０２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータ

から、秘密復号鍵Ｋｍにより復号処理をすることにより、セッションキーＫｓを抽出する復号処理部１４０４と、データバスＢＳ３から、公開暗号化鍵Ｋｐで暗号化されているコンテンツキーＫｃおよびコンテンツキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納するためのメモリ１４１２と、復号処理部１４０４により抽出されたセッションキーＫｓに基づいて、メモリ１４１２からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４０６と、メモリカード１２０の動作を制御するためのコントローラ１４２０とを備える。

なお、図６のメモリカード１２０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

［再生処理］

図７は、携帯電話機２００内において、メモリカード１２０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図７を参照して、携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストがメモリカード１２０に対して出力される（ステップＳ２００）。

メモリカード１２０においては、この再生リクエストに応じて、コントローラ１４２０は、ＫＰｍ保持部１４０１から、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、公開暗号化鍵ＫＰｍを携帯電話機２００に対して送信する（ステップＳ２０２）。

携帯電話機２００では、カード１２０からのキーＫＰｍを受信すると（ステップＳ２０４）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成し（ステップＳ２０６）、暗号化処理部１５０４が、キーＫＰｍにより、セッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］ＫＰｍを生成し、データバスＢＳ２を介して、カード１２０に対して送信する（ステップＳ２０８）。

メモリカード１２０は、携帯電話機２００により生成された暗号化セッション

キー［Ｋｓ］ＫＰｍを受け取り、復号処理部１４０４において秘密復号鍵Ｋｍにより復号し、セッションキーＫｓを抽出する（ステップＳ２１０）。

続いて、メモリカード１２０は、メモリ１４１２から、コンテンツキー［Ｋｃ］Ｋｐを読出す（ステップＳ２１２）。

続いて、メモリカード１２０は、暗号化処理部１４０６において抽出したセッションキーＫｓにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓをデータバスｂｓ２に与える（ステップＳ２１４）。

携帯電話機２００の復号処理部１５０６は、メモリカード１２０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓをセッションキーｋｓにより復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを取得する（ステップＳ２１６）。

さらに、携帯電話機２００の復号処理部１５３０は、Ｋｐ保持部１５４０からのキーＫｐに基づいて、データ［Ｋｃ］Ｋｐの復号処理を行なう（ステップＳ２１８）。

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は（ステップＳ２２０）、処理は次のステップＳ２２２に進み、抽出できない場合は（ステップＳ２２０）、処理は終了する（ステップＳ２２６）。

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスｂｓ２に与える（ステップＳ２２２）。

携帯電話機２００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２２６）。

このような構成とすることで、携帯電話機２００において生成されたセッションキーに基づいてコンテンツキーを暗号化した上で、メモリカード１２０から携

帯電話機２００に送信して再生動作を行なうことが可能となる。

以上のような構成により、実施例１の携帯電話機１００の奏する効果に加えて、実施例２の携帯電話機２００においては、携帯電話機２００に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

しかも、携帯電話機とメモリカードとの間のデータの授受は、セッションキーにより暗号化された上で行なわれるので、データに対するセキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

［実施例３］

図８は、本発明の実施例３の携帯電話機３００の構成を説明するための概略ブロック図であり、実施例２の図４と対比される図である。

図８に示した実施例３の携帯電話機３００の構成と、実施例２の携帯電話機２００の構成が異なる点は、以下のとおりである。

まず、図８においては、携帯電話機３００には、携帯電話機３００により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機３００中の音楽再生モジュール１５００に与えるための着脱可能なメモリカード１３０が装着される構成となっている。

メモリカード１３０は、後に説明するように、メモリカード１３０自身でセッションキーＫｓ２を生成する点で、メモリカード１２０と異なる。

さらに、携帯電話機３００の構成では、音楽再生モジュール１５００の構成も、携帯電話機２００の構成と異なる。

すなわち、携帯電話機３００の音楽再生モジュール１５００は、メモリカード１３０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ１を乱数等により発生するセッションキー発生部１５５２と、セッションキー発生部１５５

２により生成されたセッションキーＫｓ１をメモリカード１３０からのセッションキーＫｓ２で暗号化して、データバスＢＳ２に与えるための暗号化処理部１５５４と、データバスＢＳ２によりメモリカード１３０から伝送され、公開暗号化鍵ＫＰｐおよびセッションキーＫｓ１により暗号化コンテンツキーＫｃをセッションキーＫｓ１について復号して出力する復号処理部１５５６と、コントローラ１１０６により制御されて、データバスＢＳ２により伝達された暗号化されたメモリカード１３０のセッションキー［Ｋｓ２］Ｋｐまたは復号処理部１５５６から出力された暗号化コンテンツキー［Ｋｃ］Ｋｐのいずれかを、公開暗号化鍵ＫＰｐにより暗号化されたデータを復号するための復号処理部１５３０に与える切換え回路１５５０とを含む。

暗号化処理部１５５４は、復号処理部１５３０において秘密復号鍵Ｋｐにより復号されて抽出されたメモリカード１３０のセッションキーＫｓ２を受けて、セッションキー発生部１５５２により生成されたセッションキーＫｓ１をセッションキーＫｓ２で暗号化処理する。

携帯電話機３００のその他の部分は、実施例２の携帯電話機２００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図８においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図８に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２および切換え回路１５５０を、ＴＲＭに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機３００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図８において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータついても、保護

することが可能である。

［暗号／復号鍵の構成］

図９は、図８に示した携帯電話機３００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図８に示した構成において、メモリカード１３０内のデータ処理を管理するための鍵としては、メモリカードに固有な公開暗号化鍵ＫＰｍと、公開暗号化鍵ＫＰｍにより暗号化されたデータを復号するためのキーＫＰｍとは非対称な秘密復号鍵Ｋｍと、メモリカード１３０が生成し各セッションに固有なセッションキーＫｓ２とがある。

したがって、メモリカード１３０と携帯電話機３００とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵Ｋｍ、復号鍵ＫＰｍ、セッションキーＫｓ２が用いられることになる。

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵であって、コンテンツデータの配信時にコンテンツデータとともに配信され、後に説明するようにメモリカード１３０内に記憶される公開暗号鍵ＫＰｐと、音楽再生モジュールの管理の鍵として、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、各アクセスごとにセッションキー発生器１５５２において生成される共通鍵であるセッションキーＫｓ１とが用いられる。

セッションキーＫｓ１も各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

さらに、メモリカード１３０に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、このコンテンツキーＫｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

また、配信サーバ１０から携帯電話機３００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも公開暗号化鍵ＫＰｐにより暗号化されており、メモリカード１３０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｐとして格納されているものとする。

さらに、著作権の存在するコンテンツデータＤｃは、このコンテンツデータをコンテンツキーＫｃで復号化可能な暗号化コンテンツデータ［Ｄｃ］Ｋｃとしてメモリカード１３０に格納されているものとする。

［メモリカードの構成］

図１０は、図８に示したメモリカード１３０の構成を説明するための概略ブロック図である。

メモリカード１３０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、セッション毎にセッションキーＫｓ２を生成するためのセッションキー発生部１４５０と、セッションキーＫｓ２を公開暗号化鍵ＫＰｐで暗号化してデータバスＢＳ３に与えるための暗号化処理部１４５２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータ［Ｋｓ１］Ｋｓ２から、セッションキーＫｓ２により復号処理をすることにより、携帯電話機３００からのセッションキーＫｓ１を抽出する復号処理部１４５４と、データバスＢＳ３から、公開暗号化鍵ＫＰｐと、公開暗号化鍵ＫＰｐで暗号化されているコンテンツキー［Ｋｃ］Ｋｐとコンテンツキーにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃとの３つを受けて格納するためのメモリ１４１２と、復号処理部１４５４により抽出されたセッションキーＫｓ１に基づいて、メモリ１４１２からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４５６と、メモリカード１３０の動作を制御するためのコントローラ１４２０とを備える。

なお、図１０のメモリカード１３０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

［再生処理］

図１１は、携帯電話機３００内において、メモリカード１３０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１１を参照して、携帯電話機のキーボード１１０８等からのユーザの指示に

より、再生リクエストがメモリカード１３０に対して出力される（ステップＳ３００）。

メモリカード１３０においては、この再生リクエストに応じて、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ３０２）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機３００に対して送信する（ステップＳ３０４）。

携帯電話機３００では、カード１３０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ３０６）。

携帯電話機３００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ３０８）、暗号化処理部１５５４が、ステップＳ３０６において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化して暗号化セッションキー［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１３０に対して送信する（ステップＳ３１０）。

メモリカード１３０は、携帯電話機３００により生成され、かつ暗号化されたセッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ３１２）。

続いて、メモリカード１３０は、メモリ１４１２から、暗号化コンテンツキー［Ｋｃ］Ｋｐを読出し（ステップＳ３１４）、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ３１６）。

携帯電話機３００の復号処理部１５５６は、メモリカード１３０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１に対してセッショ

ンキーＫｓ１により復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを取得する（ステップＳ３１８）。

さらに、携帯電話機３００の復号処理部１５３０は、切換え回路１５５０を介して暗号化コンテンツキー［Ｋｃ］Ｋｐを受け、Ｋｐ保持部１５４０からのキーＫｐに基づいて、暗号化コンテンツキー［Ｋｃ］Ｋｐの復号処理を行なう（ステップＳ３２０）。

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は（ステップＳ３２２）、処理は次のステップＳ３２４に進み、抽出できない場合は（ステップＳ３２２）、処理は終了する（ステップＳ３３０）。

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１３０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ３２４）。

携帯電話機３００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し（ステップＳ３２８）、処理が終了する（ステップＳ３３０）。

このような構成とすることで、携帯電話機３００において生成されたセッションキーＫｓ１に基づいて暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化した上で、メモリカード１３０から携帯電話機３００に送信して再生動作を行なうことが可能となる。しかも、メモリカード１３０においてセッション毎に生成されたセッションキーＫｓ２により暗号化した上で、メモリカード１３０と携帯電話機３００との間でセッションキーＫｓ１の授受が行なわれるので、実施例２よりも一層、セキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

また、以上のような構成により、実施例３の携帯電話機３００においても、携帯電話機３００に対して、着脱可能なメモリカード内に配信データが格納される

構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

［実施例４］

図１２は、本発明の実施例４の携帯電話機４００の構成を説明するための概略ブロック図であり、実施例３の図８と対比される図である。

図１２に示した実施例４の携帯電話機４００の構成と、実施例３の携帯電話機３００の構成が異なる点は、以下のとおりである。

すなわち、図１２においては、携帯電話機４００には、携帯電話機４００により受信された暗号化コンテンツデータおよび暗号化コンテンツキーを受取って格納し、さらに所定の暗号化処理をした上で、携帯電話機４００中の音楽再生モジュール１５００に与えるための着脱可能なメモリカード１４０が装着される構成となっている。メモリカード１４０は、後に説明するように、携帯電話機４００に対する認証機能を有する点で実施例３のメモリカード１３０と異なる。

さらに、携帯電話機４００の構成では、音楽再生モジュール１５００の構成も、携帯電話機３００の構成と異なる。

すなわち、携帯電話機４００の音楽再生モジュール１５００は、メモリカード１４０と携帯電話の他の部分とのデータ授受にあたり、携帯電話機４００に対する認証機能を実現するために、再生装置である携帯電話機４００のクラス（種類等）に固有な公開暗号鍵ＫＰｐと認証データＣｒｔｆとを、システムに共通な公開復号鍵（公開認証鍵）ＫＰｍａにより暗号化して保持する［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０をさらに備える構成となっている点である。

携帯電話機４００のその他の部分は、実施例３の携帯電話機３００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図１２においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図１２に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２、切換え回路１５５０および［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０を、ＴＲＭに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機４００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図１２において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータついても、保護することが可能である。

［暗号／復号鍵の構成］

図１３は、図１２に示した携帯電話機４００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図１２に示した構成において、メモリカード１４０内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵であり、認証鍵の機能を有するＫＰｍａと、メモリカード１４０が生成し各セッションに固有な共通鍵であるセッションキーＫｓ２とがある。

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のクラスに固有な公開暗号化鍵であって、上述のとおり、鍵ＫＰｍａにより暗号化された形で携帯電話機４００中の［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０に格納されている公開暗号鍵ＫＰｐと、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、各アクセスごとにセッションキー発生器１５５２において生成される共通鍵でるセッションキーＫｓ１とが用いられる。

セッションキーＫｓ１も各通信セッションに固有の値を有することになり、音

楽再生モジュール１５００において管理される。

なお、「再生装置のクラス」とは、再生装置ごと、あるいは、再生装置の種類（製造メーカ、製造ロット）ごとに、この再生装置を区別するための区分であるものとする。

さらに、メモリカード１４０に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、このコンテンツキーＫｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

また、配信サーバ１０から携帯電話機４００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも公開暗号化鍵ＫＰｐにより暗号化されており、メモリカード１４０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｐとして格納されているものとする。

さらに、著作権の存在するコンテンツデータＤｃは、このコンテンツデータをコンテンツキーＫｃで復号化可能な暗号化コンテンツデータ［Ｄｃ］Ｋｃとしてメモリカード１４０に格納されているものとする。

［メモリカードの構成］

図１４は、図１２に示したメモリカード１４０の構成を説明するための概略ブロック図である。

メモリカード１４０の構成が、実施例３のメモリカード１３０の構成と異なる点は、まず、コントローラ１４２０に制御されて、データバスＢＳ３上のデータに対して公開復号鍵ＫＰｍａによる復号処理を行い、携帯電話機１４０からの公開暗号鍵ＫＰｐおよび認証データＣｒｔｆの取得を行うための復号処理部１４６０を備える構成となっている点である。したがって、暗号化処理部１４５２は、復号処理部１４６０からの公開暗号化鍵ＫＰｐに基づいて暗号化処理を行う。

さらに、メモリカード１４０中のメモリ１４１２においては、メモリカード１３０の場合に保持されていた公開暗号化鍵ＫＰｐの代わりに、公開復号鍵ＫＰｍａが格納されている。したがって、復号処理部１４６０は、メモリ１４１２中に保持された公開復号鍵ＫＰｍａに基づいて復号処理を行う。

メモリカード１４０のその他の部分は、実施例３のメモリカード１３０の構成

と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図１４のメモリカード１４０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内の鍵等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

［再生処理］

図１５は、携帯電話機４００内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

図１５を参照して、再生処理の説明を行なう。携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストが与えられると（ステップＳ４００）、携帯電話機４００の［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａ保持部１５６０からメモリカード１４０に対してデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａが出力される（ステップＳ４０２）。

メモリカード１４０においては、このデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａを復号部１４６０により復号し、公開暗号化鍵ＫＰｐと認証データＣｒｔｆとを獲得する（ステップＳ４０６）。コントローラ１４２０は、認証データＣｒｔｆに基づいて携帯電話機４００の認証を行ない（ステップＳ４０６）、携帯電話機４００が正規の機器であれば処理をステップＳ４０８に移行し、携帯電話機４００が正規の機器でない場合、再生のための動作を行なわずに処理を終了する（ステップＳ４３４）。

携帯電話機４００が正規の機器である場合、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ４０８）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機４００に対して送信する（ステップＳ４１０）。

携帯電話機４００では、カード１４０からの暗号化セッションキー［Ｋｓ２］

Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ４１２）。

携帯電話機４００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ４１４）、暗号化処理部１５５４が、ステップＳ４１２において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化してデータ［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１４０に対して送信する（ステップＳ４１６）。

メモリカード１４０は、携帯電話機４００により生成され、かつ暗号化されたセッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ４１８）。

続いて、メモリカード１４０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ］Ｋｐを読出し（ステップＳ４２０）、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ４２２）。

携帯電話機４００の復号処理部１５５６は、メモリカード１４０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１に対してセッションキーＫｓ１により復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを取得する（ステップＳ４２４）。

さらに、携帯電話機４００の復号処理部１５３０は、切換え回路１５５０を介して暗号化コンテンツキー［Ｋｃ］Ｋｐを受け、Ｋｐ保持部１５４０からのキーＫｐに基づいて、データ［Ｋｃ］Ｋｐの復号処理を行なう（ステップＳ４２６）。

復号処理部１５３０が、復号処理によりコンテンツキーＫｃを抽出できた場合は（ステップＳ４２８）、処理は次のステップＳ４３０に進み、抽出できない場合は（ステップＳ４２８）、処理は終了する（ステップＳ４３４）。

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４

１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ４３０）。

携帯電話機４００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文の音楽データＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップＳ４３２）、処理が終了する（ステップＳ４３４）。

このような構成とすることで、実施例３の携帯電話機３００およびメモリカード１３０の奏する効果に加えて、携帯電話機４００からのデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａに基づいて、メモリカード１４０が認証の結果、正規の機器と判断された携帯電話機４００とメモリカード１４０の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

［実施例５］

図１６は、本発明の実施例５の携帯電話機５００の構成を説明するための概略ブロック図であり、実施例４の図１２と対比される図である。

図１６に示した実施例５の携帯電話機５００の構成と、実施例４の携帯電話機４００の構成が異なる点は、以下のとおりである。

すなわち、図１６においては、メモリカード１４０に代わりメモリカード１５０が装着されており、さらに、メモリカード１５０から携帯電話機５００に対してコンテンツキーＫｃを送信する場合は、セッションキーＫｓ１により暗号化されたデータ［Ｋｃ］Ｋｓ１として送信される。したがって、実施例４の場合のように、コンテンツキーＫｃの送信の際に、キーＫＰｐとキーＫｓ１により２重に暗号化されているわけではないため、キーＫｓ１による復号処理とキーＫｐによる復号処理とは、独立に行なうことが可能となり、図１６に示した携帯電話機５００においてはにおいては切換スイッチ１５５０が省略されている。

すなわち、携帯電話機５００の音楽再生モジュール１５００は、秘密復号鍵Ｋｐを保持するためのＫｐ保持部１５４０と、メモリカード１５０からデータバス

Ｂｓ２を介して与えられるデータ［Ｋｓ２］ＫｐをキーＫｐにより復号化するための復号処理部１５３０と、メモリカード１５０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ１を乱数等により発生するセッションキー発生部１５５２と、セッションキー発生部１５５２により生成されたセッションキーＫｓ１をメモリカード１５０からのセッションキーＫｓ２で暗号化して、データバスＢＳ２に与えるための暗号化処理部１５５４と、データバスＢＳ２によりメモリカード１５０から伝送され、セッションキーＫｓ１により暗号化コンテンツキーＫｃをセッションキーＫｓ１について復号して出力する復号処理部１５５６と、復号処理部１５５６から出力されるコンテンツキーＫｃに基づいて、データバスＢｓ２を介してメモリカード１５０から与えられる暗号化コンテンツデータ［Ｄｃ］Ｋｃを復号して音楽再生部１５０８に与えるための復号処理部１５２０と、メモリカード１５０と携帯電話の他の部分とのデータ授受にあたり、携帯電話機５００に対する認証機能を実現するために、再生装置である携帯電話機５００のクラス（種類等）に固有な公開暗号鍵ＫＰｐと認証データＣｒｔｆとを、システムに共通な公開復号鍵ＫＰｍａにより暗号化して保持する［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０とを備える。

携帯電話機５００のその他の部分は、実施例４の携帯電話機４００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図１６においても、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図１６に示した構成においても、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２および［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０を、ＴＲＭに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機５００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキ

ュリティが向上する。

さらに、図１６において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータついても、保護することが可能である。

［メモリカードの構成］

図１７は、図１６に示したメモリカード１５０の構成を説明するための概略ブロック図である。

メモリカード１５０の構成が、実施例４のメモリカード１４０の構成と異なる点は、コンテンツキーＫｃがメモリ１４１２中に暗号化されることなく、平分データとして格納されている点である。

メモリカード１５０のその他の部分は、実施例４のメモリカード１４０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図１７のメモリカード１５０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とする。

［再生処理］

図１８は、携帯電話機５００内において、メモリカード１５０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１８を参照して、再生処理についての説明を行なう。携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストが与えられると（ステップＳ５００）、携帯電話機５００の［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａ保持部１５６０からメモリカード１５０に対してデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａが出力される（ステップＳ５０２）。

メモリカード１５０においては、このデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａを復号部１４６０により復号し、公開暗号化鍵ＫＰｐと認証データＣｒｔｆとを獲得する（ステップＳ５０６）。コントローラ１４２０は、認証データＣｒｔｆに

基づいて携帯電話機５００の認証を行ない（ステップＳ５０６）、携帯電話機５００が正規の機器であれば処理をステップＳ５０８に移行し、携帯電話機５００が正規の機器でない場合、再生のための動作を行なわずに処理を終了する（ステップＳ５３４）。

携帯電話機５００が正規の機器である場合、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ５０８）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機５００に対して送信する（ステップＳ５１０）。

携帯電話機５００では、カード１５０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ５１２）。

携帯電話機５００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ５１４）、暗号化処理部１５５４が、ステップＳ５１２において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化してデータ［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１５０に対して送信する（ステップＳ５１６）。

メモリカード１５０は、携帯電話機５００により生成され、かつ暗号化されたセッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ５１８）。

続いて、メモリカード１５０は、メモリ１４１２から、コンテンツキーＫｃを読出す（ステップＳ５２０）。

続いて、メモリカード１５０は、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、コンテンツキーＫｃを暗号化し、暗号化コンテンツキー［Ｋｃ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える

（ステップＳ５２２）。

携帯電話機５００の復号処理部１５５６は、メモリカード１５０から送信された暗号化された暗号化コンテンツキー［Ｋｃ］Ｋｓ１に対して、セッションキーＫｓ１により復号処理を行なうことにより、コンテンツキーＫｃを取得する（ステップＳ５２４）。

メモリカード１５０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ５３０）。

携帯電話機５００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し（ステップＳ５３２）、処理が終了する（ステップＳ５３４）。

このような構成とすることで、実施例４の携帯電話機４００およびメモリカード１３０の奏する効果と同様に、携帯電話機５００からのデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａに基づいて、メモリカード１５０が認証の結果、正規の機器と判断された携帯電話機５００とメモリカード１５０の間でしか再生動作が行なわれないため、著作権者の著作権の保護を図ることが、より簡易な構成で可能となる。

［実施例６］

図１９は、本発明の実施例６の携帯電話機６００の構成を説明するための概略ブロック図であり、実施例５の図１６と対比される図である。

図１９に示した実施例６の携帯電話機６００の構成と、実施例５の携帯電話機５００の構成が異なる点は、以下のとおりである。

すなわち、図１９においては、携帯電話機６００は、システム共通の秘密復号鍵Ｋｃｏｍを保持するためのＫｃｏｍ保持部１５７０と、復号処理部１５５６の出力を受けて、秘密復号鍵Ｋｃｏｍにより復号してコンテンツキーＫｃを獲得し、復号処理部１５２０に与える復号処理部１５７２をさらに備える構成となっている。

すなわち、実施例５においては、メモリカード１５０から携帯電話機５００に対してコンテンツキーＫｃを送信する場合は、セッションキーＫｓ１により暗号化されたコンテンツキー［Ｋｃ］Ｋｓ１として送信されたのに対し、実施例６においては、メモリカード１６０から携帯電話機６００に対してコンテンツキーＫｃを送信する場合は、秘密復号鍵ＫｃｏｍおよびセッションキーＫｓ１により復号可能なように暗号化されたコンテンツキー［［Ｋｃ］Ｋｃｏｍ］Ｋｓ１として送信される。

携帯電話機６００のその他の部分は、実施例５の携帯電話機５００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図１９においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図１９に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２、［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０、Ｋｃｏｍ保持部および復号処理部１５７２を、ＴＲＭに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたコンテンツデータを外部から不正に取得することができなくなり、セキュリティが向上する。

さらに、図１９において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータついても、保護することが可能である。

［暗号／復号鍵の構成］

図２０は、図１９に示した携帯電話機６００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図１９に示した構成において、メモリカード１６０内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵ＫＰｍａと、メモリカー

ド１６０が生成し各セッションに固有なセッションキーＫｓ２とがある。

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のクラスに固有な公開暗号化鍵であって、鍵ＫＰｍａにより暗号化された形で携帯電話機６００中の［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０に格納されている公開暗号鍵ＫＰｐと、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、システムに共通な秘密復号鍵Ｋｃｏｍと、各アクセスごとにセッションキー発生器１５５２において生成される共通鍵であるセッションキーＫｓ１とが用いられる。

セッションキーＫｓ１も各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

さらに、メモリカード１６０に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、この共通鍵Ｋｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

また、配信サーバ１０から携帯電話機６００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも秘密復号鍵Ｋｃｏｍにより復号可能なように暗号化されており、メモリカード１６０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍとして格納されているものとする。

さらに、著作権の存在するコンテンツデータＤｃは、このコンテンツデータをコンテンツキーＫｃで復号化可能な暗号化コンテンツデータ［Ｄｃ］Ｋｃとしてメモリカード１６０に格納されているものとする。

［メモリカードの構成］

図２１は、図１９に示したメモリカード１６０の構成を説明するための概略ブロック図である。

メモリカード１６０の構成が、実施例５のメモリカード１５０の構成と異なる点は、コンテンツキーＫｃがメモリ１４１２中においては、暗号化データ［Ｋｃ］Ｋｃｏｍとして格納されている点である。

メモリカード１６０のその他の部分は、実施例５のメモリカード１５０の構成

と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図２１のメモリカード１６０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

［再生処理］

図２２は、携帯電話機６００内において、メモリカード１６０に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

図２２を参照して、携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストが与えられると（ステップＳ６００）、携帯電話機６００の［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａ保持部１５６０からメモリカード１６０に対してデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａが出力される（ステップＳ６０２）。

メモリカード１６０においては、このデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａを復号部１４６０により復号し、公開暗号化鍵ＫＰｐと認証データＣｒｔｆとを獲得する（ステップＳ６０６）。コントローラ１４２０は、認証データＣｒｔｆに基づいて携帯電話機６００の認証を行ない（ステップＳ６０６）、携帯電話機６００が正規の機器であれば処理をステップＳ６０８に移行し、携帯電話機６００が正規の機器でない場合、再生のための動作を行なわずに処理を終了する（ステップＳ６３４）。

携帯電話機６００が正規の機器である場合、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ６０８）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機６００に対して送信する（ステップＳ６１０）。

携帯電話機６００では、カード１６０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セ

ッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ６１２）。

携帯電話機６００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ６１４）、暗号化処理部１５５４が、ステップＳ６１２において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化して暗号化セッションキー［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１６０に対して送信する（ステップＳ６１６）。

メモリカード１６０は、携帯電話機６００により生成された暗号化セッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ６１８）。

続いて、メモリカード１６０は、メモリ１４１２から、暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを読出す（ステップＳ６２０）。

続いて、メモリカード１６０は、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｃｏｍ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ６２２）。

携帯電話機６００の復号処理部１５５６は、メモリカード１６０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｃｏｍ］Ｋｓ１に対してセッションキーＫｓ１により復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを取得する（ステップＳ６２４）。

さらに、携帯電話機６００の復号処理部１５７２は、復号処理部１５５６から暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを受け、Ｋｃｏｍ保持部１５７０からのキーＫｃｏｍに基づいて、データ［Ｋｃ］Ｋｃｏｍの復号処理を行なう（ステップＳ６２６）。

復号処理部１５７２が、復号処理によりコンテンツキーＫｃを抽出できた場合は（ステップＳ６２８）、処理は次のステップＳ６３０に進み、抽出できない場合は（ステップＳ６２８）、処理は終了する（ステップＳ６３４）。

復号処理部１５７２が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１６０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４

１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ６３０）。

携帯電話機６００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップＳ６３２）、処理が終了する（ステップＳ６３４）。

このような構成とすることで、実施例４の携帯電話機４００およびメモリカード１４０の奏する効果と同様に、携帯電話機６００からのデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａに基づいて、メモリカード１６０が認証の結果、正規の機器と判断された携帯電話機６００とメモリカード１６０の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

１．暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（１００）であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部（１１０、１２０、１３０）と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部（１５００）とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツキーを復号するための第１の復号鍵を保持する第１の鍵保持部（１５４０）と、

前記データ格納部からの前記暗号化コンテンツキーを基にして、前記第１の鍵保持部からの出力により復号処理を行なうことで、前記コンテンツキーを抽出する第１の復号処理部（１５３０）と、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、前記第１の復号処理部の出力により復号してコンテンツデータを抽出するための第２の復号処理部（１５２０）とを含む、データ再生装置。

２．前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスする毎に更新される第１のセッションキーを生成する第１のセッションキー発生部（１５０２）と、

前記第１のセッションキーを前記データ格納部にて復号可能な第１の暗号鍵で暗号化して前記データ格納部に与えるための第１の暗号化処理部（１５０４）と、

前記第１のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第１のセッションキーについて復号して前記第１の復号処理部に与える第３の復号処理部（１５０６）をさらに含む、請求項１記載のデータ再生装置。

３．前記コンテンツデータは、データ量を削減するための符号化方式にて符号化

された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部（１５０８）と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（１５１２）とをさらに含む、請求項２に記載のデータ再生装置。

４．前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項３に記載のデータ再生装置。

５．前記データ格納部（１２０）は、

前記データ格納部に与えられるデータを保持するための記憶部（１４１２）と、

前記第１の暗号化鍵を保持する第２の鍵保持部（１４０１）と、

前記第１の暗号化鍵により暗号化されたデータを復号するための第２の復号鍵を保持するための第３の鍵保持部（１４０２）と、

前記第２の復号鍵に基づいて、前記データ再生部から前記第１の暗号化鍵により暗号化されて伝達された前記第１のセッションキーを復号するための第４の復号処理部（１４０４）と、

前記第４の復号処理部で抽出された前記第１のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第２の暗号化処理部（１４０６）とを備える、請求項２記載のデータ再生装置。

６．前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項５記載のデータ再生装置。

７．前記データ再生部は、前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに異なる第２のセッションキーを、さらに、前記第１の復号鍵により復号可能な暗号化を施して供給を受け、

前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに更新される第１のセッションキーを生成する第１のセッションキー発生部（１５５２）と、

前記第１のセッションキーを、外部から入力されたデータから前記第１の復号

鍵に基づいて前記第１の復号処理部にて抽出された前記第２のセッションキーで暗号化して前記データ格納部に与えるための第２の暗号処理部（１５５４）と、

前記第１のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第１のセッションキーについて復号して前記第１の復号処理部に与える第３の復号処理部（１５５６）をさらに含む、請求項１記載のデータ再生装置。

８．前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項７に記載のデータ再生装置。

９．前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項８項に記載のデータ再生装置。

１０．前記データ格納部（１３０）は、

前記データ格納部に与えられるデータを保持するための記録部（１４１２）と、

前記暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第２のセッションキーを発生する第２のセッションキー発生部（１４５０）と、

前記第１の復号鍵にて復号可能な第２の暗号化鍵により、暗号化処理を行なう第３の暗号化処理部（１４５２）と、

前記第２のセッションキーに基づいて、前記データ再生部から前記第２のセッションキーにて暗号化されて伝達された前記第１のセッションキーを復号するための第５の復号処理手段（１４５４）と、

前記第５の復号処理手段にて抽出された前記第１のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第４の暗号化処理部（１４５６）とを備える、請求項７記載のデータ再生装置。

１１．前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項１０記載のデータ再生装置。

１２．前記データ再生部は、

少なくとも前記第１の鍵保持部と、前記第１の復号処理部と、前記第２の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている、請求項１記載のデータ再生装置。

１３．暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを保持し、かつ、前記データ再生装置に着脱可能なデータ格納部（１４０、１５０、１６０）と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部（１５００）とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、復号してコンテンツデータを抽出するための第１の復号処理部（１５２０）と、

認証データを認証鍵により復号可能な暗号化を施して保持し前記データ格納部に対して出力可能な認証データ保持部（１５６０）とを含み、

前記データ格納部は、

前記認証鍵により暗号化されて前記データ再生部から与えられる前記認証データを復号して抽出するための第２の復号処理部（１４６０）と、

前記第２の復号処理部により抽出された前記認証データに基づいて認証処理を行う制御手段（１４２０）とを含む、データ再生装置。

１４．前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツキーの取得のためにアクセスする毎に更新される第１のセッションキーを生成するセッションキー発生部（１５５２）と、

前記セッションキーを前記データ格納部にて復号可能な第１の暗号鍵で暗号化して前記データ格納部に与えるための暗号化処理部（１５５４）と、

前記第１のセッションキーで暗号化されて前記データ格納部から受信した前記暗号化コンテンツキーを、前記第１のセッションキーについて復号する第３の復

号処理部（１５５６）とをさらに含む、請求項１３記載のデータ再生装置。

１５．前記第３の復号処理部は、復号結果を前記暗号化コンテンツデータを復号するためのコンテンツキーとして前記第１の復号処理部に与える、請求項１４記載のデータ再生装置。

１６．前記認証データ保持部は、第１の復号鍵で復号可能な暗号化を施すための第２の暗号鍵を前記認証データとともに前記認証鍵により復号可能な暗号化を施して保持し、前記データ格納部に対して出力し、

前記データ再生部は、前記第２の暗号鍵で暗号化された上で前記データ格納部から受信した前記第１の暗号化鍵を、前記第１の復号鍵にて復号し、前記暗号化処理部に与える第４の復号処理部（１５３０）をさらに備える、請求項１４記載のデータ再生装置。

１７．前記第４の復号処理部（１５３０）は、さらに、

前記第１の復号鍵で復号可能なように前記第２の暗号鍵で暗号化され、さらに前記第１のセッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキーを前記第３の復号処理部が前記第１のセッションキーについて復号した結果を入力として受けて、前記第２の暗号化鍵にて暗号化されたコンテンツキーを前記第１の復号鍵にて復号し、前記第１の復号処理部に与える、請求項１６記載のデータ再生装置。

１８．前記データ再生部は、

予め定められた第２復号鍵にて復号するための第５の復号処理部（１５７２）をさらに備え、

前記第５の復号処理部は、

前記第２の復号鍵で復号可能な暗号化を施されて、さらに前記第１のセッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキーを前記第３の復号部が前記第１のセッションキーについて復号した結果を入力として受け、前記第２の復号鍵にて復号し、前記第１の復号処理部に与える、請求項１４記載のデータ再生装置。

１９．前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項１３項に記載のデータ再生装置。

２０．前記データ再生装置は、さらに、簡易携帯電話網を含む携帯電話網に接続するインタフェースを備える、請求項１３に記載のデータ再生装置。

２１．前記データ再生装置は、さらに、前記インタフェースを介して通話を行なう通話処理部を備える、請求項２０記載のデータ再生装置。

２２．前記データ格納部は、前記データ再生部に対して着脱可能である、請求項２１に記載のデータ再生装置。

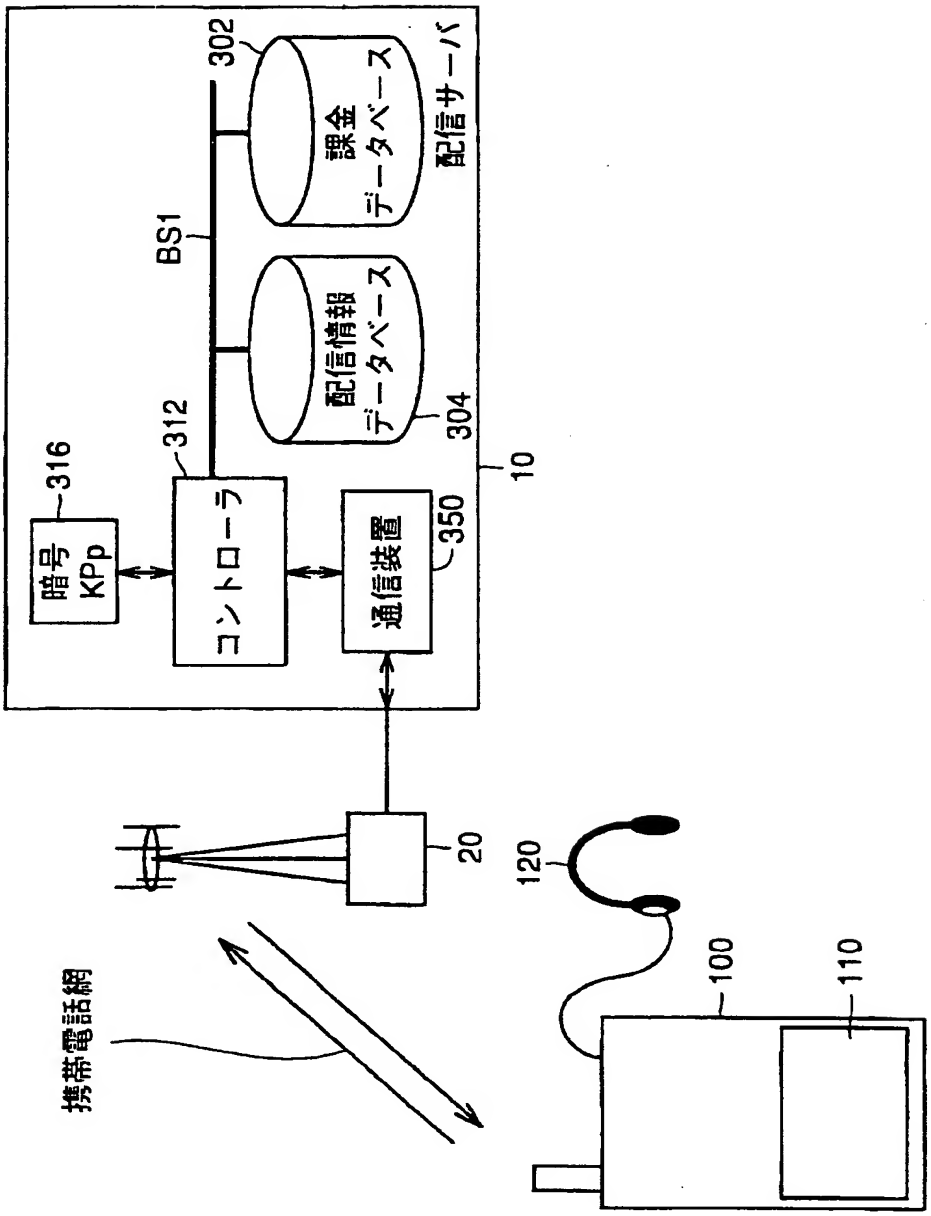

配信サーバ
10
302
課金
データベース
BS1
配信情報
データベース
304
312
316
暗号
KPp
コントローラ
通信装置
350
20
120
100
110
携帯電話網

FIG. 1

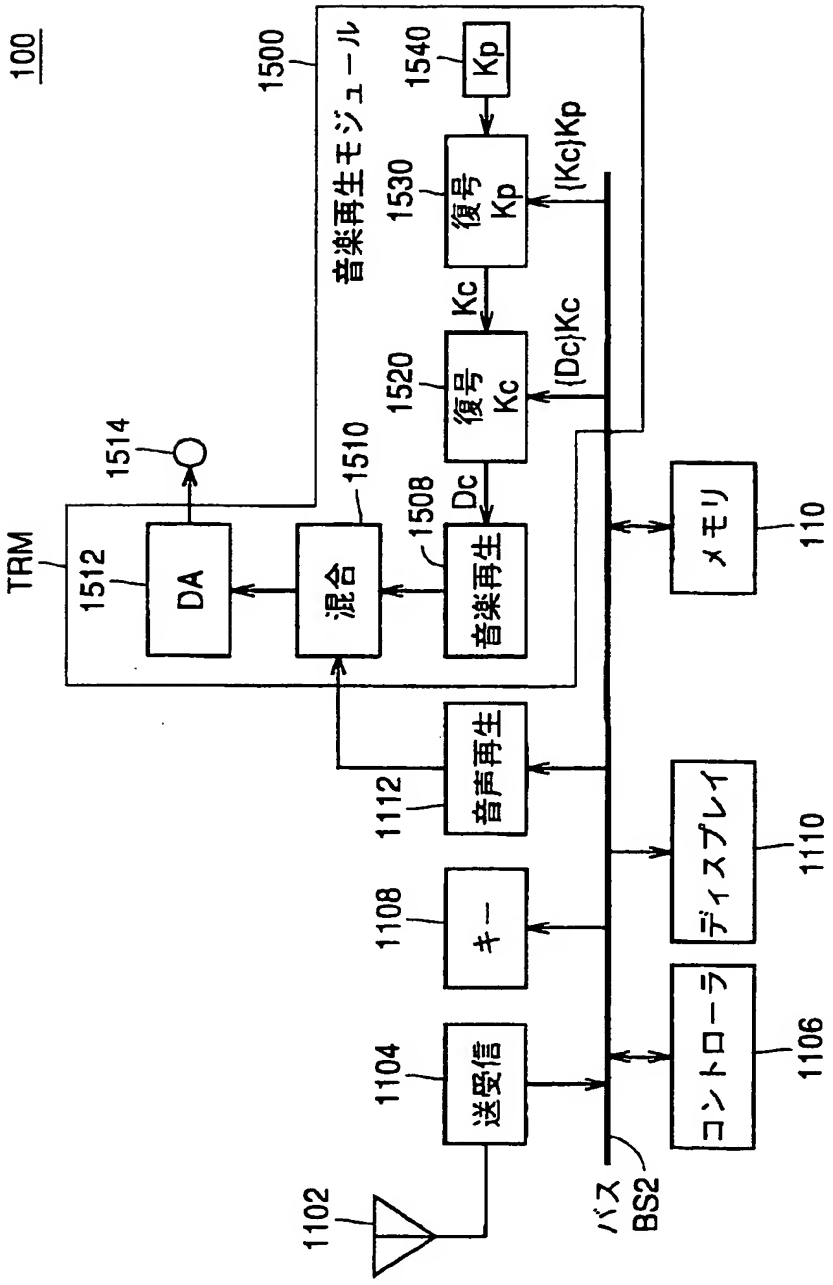

100
1500
音楽再生モジュール
1540
Kp
1530
復号 Kp
{Kc}Kp
Kc
1520
復号 Kc
{Dc}Kc
Dc
1508
音楽再生
1510
混合
1514
TRM
1512
DA
メモリ
110
音声再生
1112
キー
1108
送受信
1104
1102
ディスプレイ
1110
コントローラ
1106
バス
BS2

FIG. 2

FIG. 3

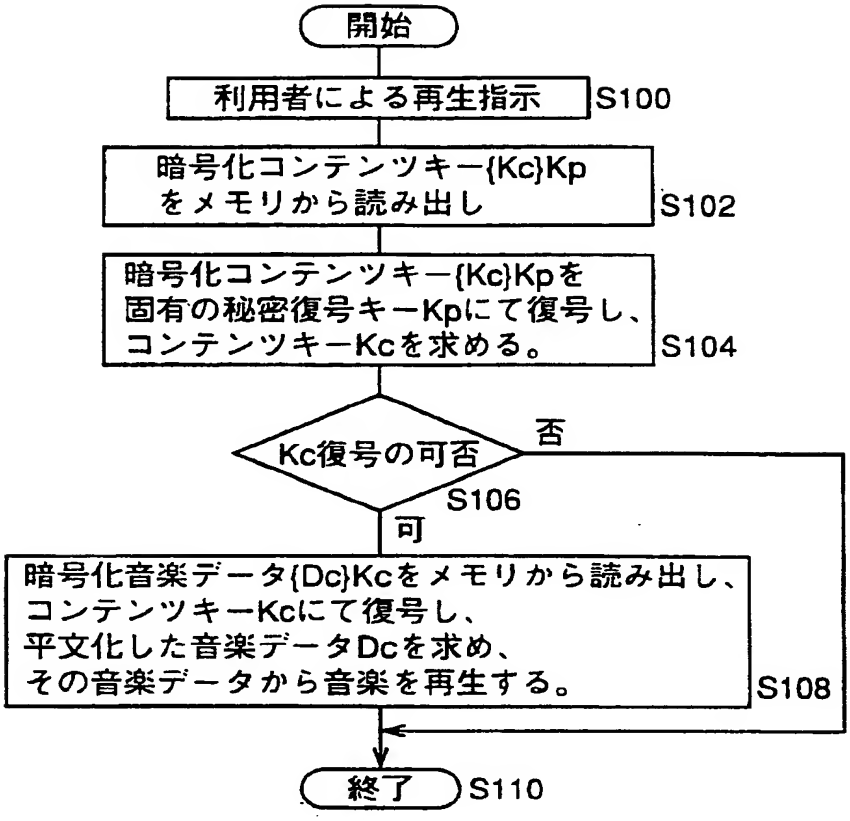

開始
利用者による再生指示
S100
暗号化コンテンツキー{Kc}Kp
をメモリから読み出し
S102
暗号化コンテンツキー{Kc}Kpを
固有の秘密復号キーKpにて復号し、
コンテンツキーKcを求める。
S104
Kc復号の可否
S106
否
可
暗号化音楽データ{Dc}Kcをメモリから読み出し、
コンテンツキーKcにて復号し、
平文化した音楽データDcを求め、
その音楽データから音楽を再生する。
S108
終了
S110

FIG. 4

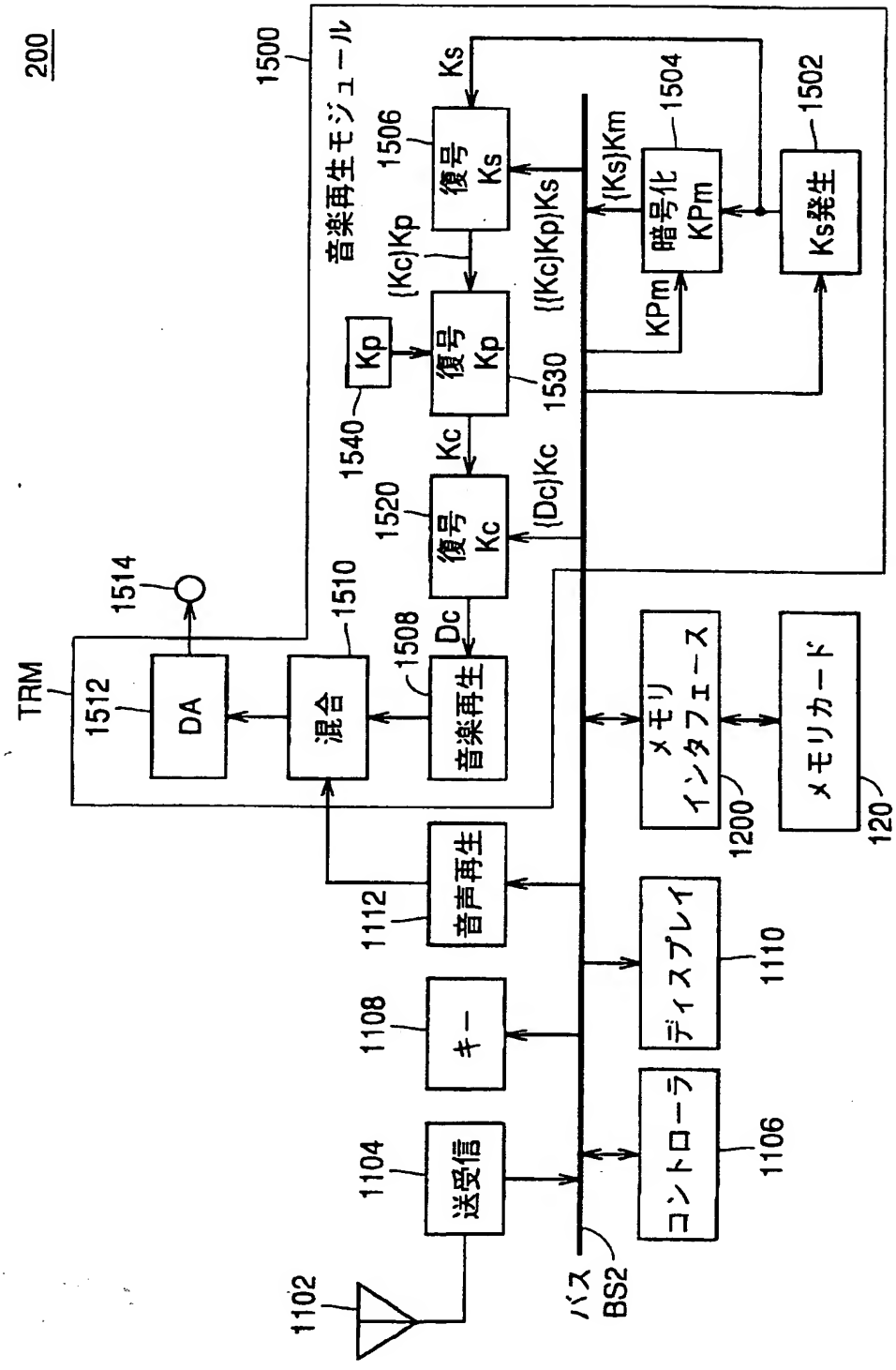

200
1500
音楽再生モジュール
TRM
1512
DA
1514
1510
混合
1508
音楽再生
Dc
1520
復号 Kc
Kc
1540
Kp
復号 Kp
1530
{Kc}Kp
1506
復号 Ks
Ks
{{Kc}Kp}Ks
{Ks}Km
1504
暗号化 KPm
KPm
1502
Ks発生
{Dc}Kc
メモリインタフェース
1200
メモリカード
120
1112
音声再生
1108
キー
1110
ディスプレイ
1104
送受信
1106
コントローラ
1102
バス BS2

FIG. 5

	記号	属性	特性	
メモリカード管理の鍵	Km	秘密復号鍵		メモリカード毎に異なる
	KPm	公開暗号鍵	Kmと対を成す	KPmで暗号化されたデータは非対称な復号鍵Kmで復号可能
音楽再生モジュール管理の鍵	Kp	秘密復号鍵	データ再生装置（携帯電話機）固有	データ再生装置毎に異なる
	Ks	共通鍵	セッション固有	メモリと音楽再生モジュール間のアクセス毎に発生
配信データ	KPp	公開暗号鍵	Kpと対を成す（Kcを暗号化）	KPpで暗号化されたデータは非対称な復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	コンテンツデータ		例：音楽データ

FIG. 6

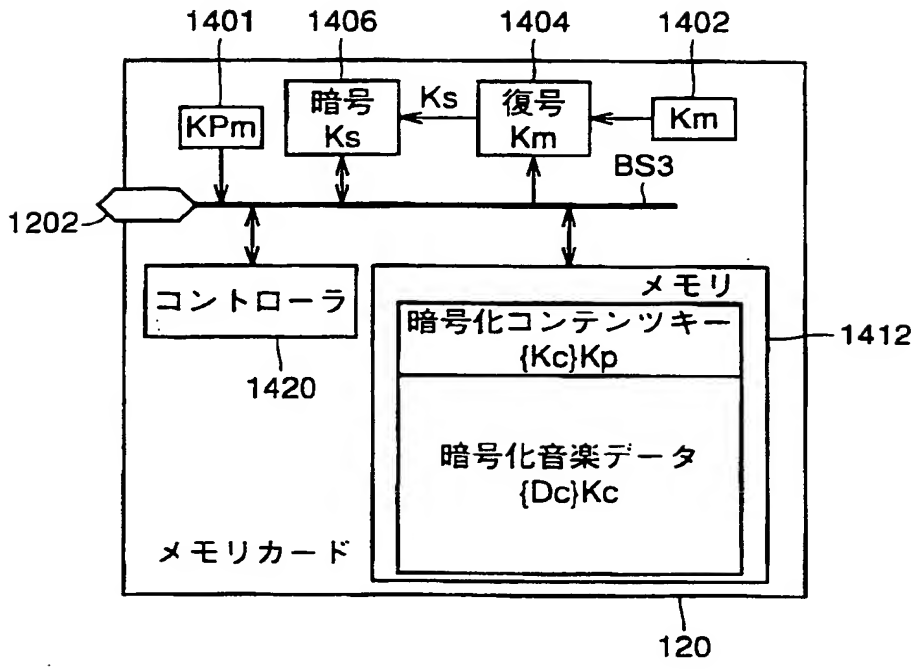
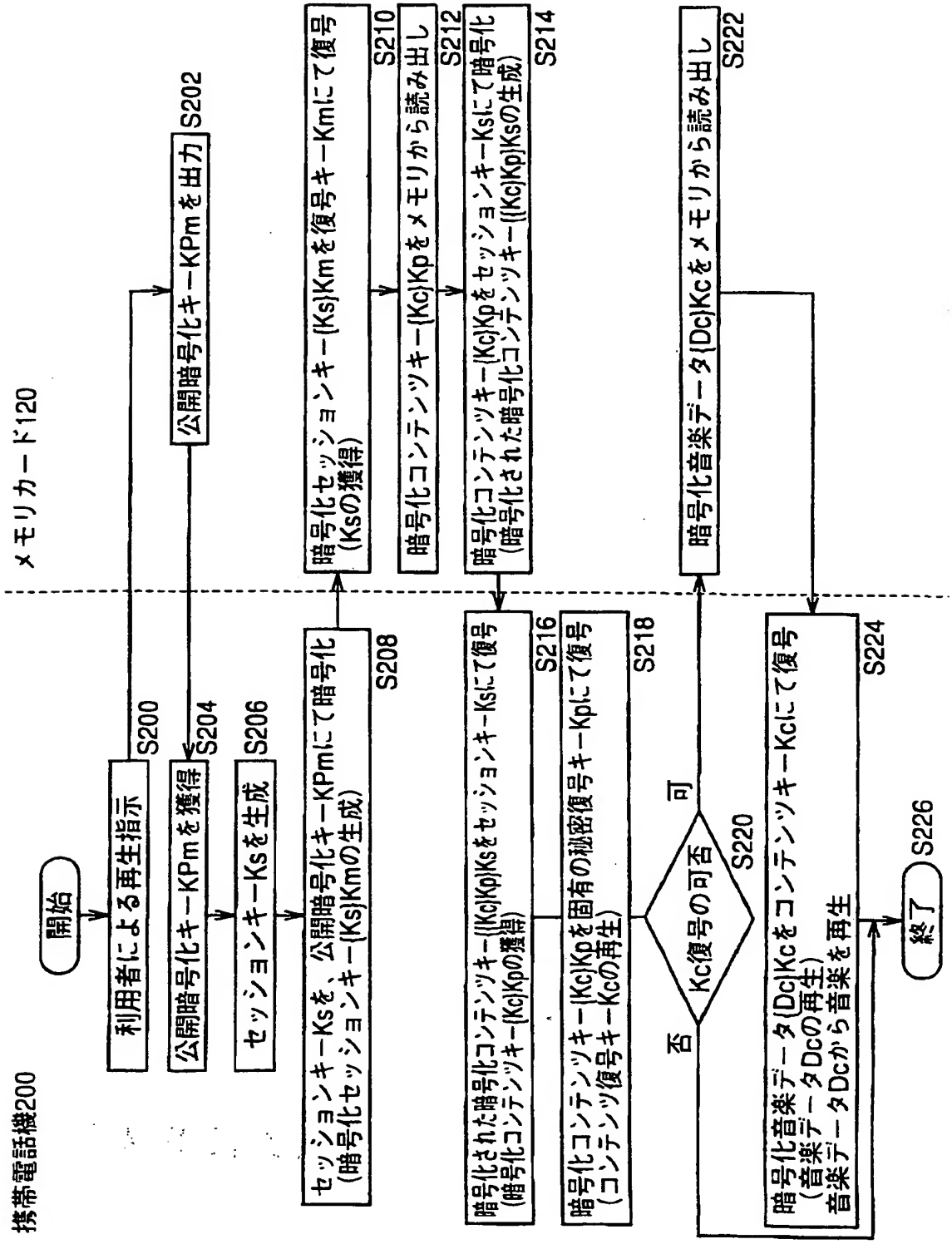

1401
1406
1404
1402
KPm
暗号
Ks
Ks
復号
Km
Km
BS3
1202
コントローラ
1420
メモリ
暗号化コンテンツキー
{Kc}Kp
暗号化音楽データ
{Dc}Kc
1412
メモリカード
120

FIG. 7


携帯電話機200
メモリカード120
開始
利用者による再生指示
S200
公開暗号化キーKPmを出力
S202
公開暗号化キーKPmを獲得
S204
セッションキーKsを生成
S206
セッションキーKsを、公開暗号化キーKPmにて暗号化
(暗号化セッションキー{Ks}Kmの生成)
S208
暗号化セッションキー{Ks}Kmを復号キーKmにて復号
(Ksの獲得)
S210
暗号化コンテンツキー{Kc}Kpをメモリから読み出し
S212
暗号化コンテンツキー{Kc}Kpをセッションキー{Ks}にて暗号化
(暗号化された暗号化コンテンツキー{{Kc}Kp}Ksの生成)
S214
暗号化された暗号化コンテンツキー{{Kc}Kp}Ksをセッションキー{Ks}にて復号
(暗号化コンテンツキー{Kc}Kpの獲得)
S216
暗号化コンテンツキー{Kc}Kpを固有の秘密復号キーKpにて復号
(コンテンツ復号キーKcの再生)
S218
Kc復号の可否
S220
否
可
暗号化音楽データ{Dc}Kcをメモリから読み出し
S222
暗号化音楽データ{Dc}Kcをコンテンツキー{Kc}にて復号
(音楽データDcの再生)
音楽データDcから音楽を再生
S224
終了
S226

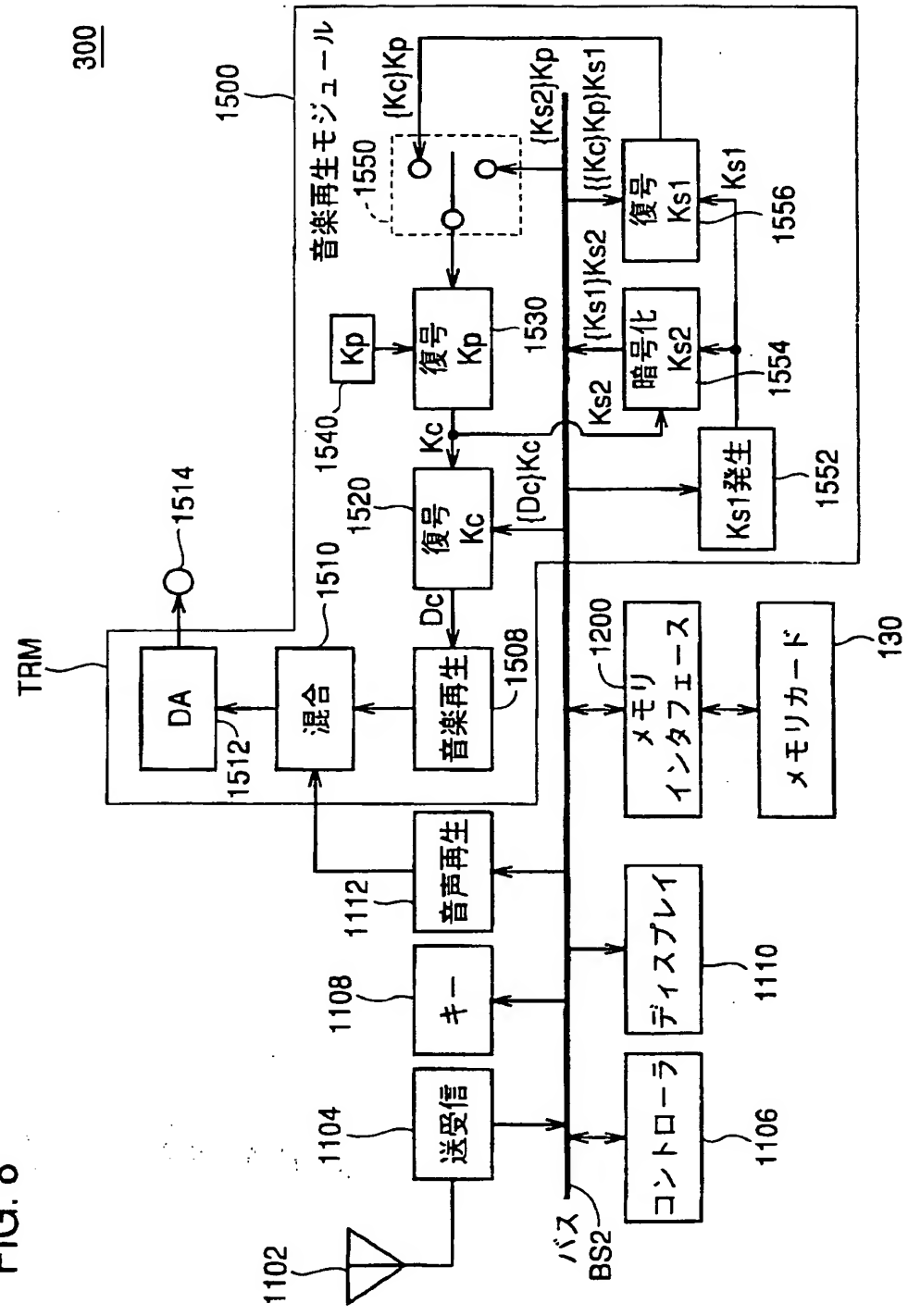

300
1500
音楽再生モジュール
TRM
1514
DA
1512
混合
1510
音楽再生
1508
復号
Kc
1520
Dc
Kc
{Dc}Kc
Kp
1540
復号
Kp
1530
{Kc}Kp
{Ks2}Kp
1550
{{Kc}Kp}Ks1
復号
Ks1
1556
Ks1
{Ks1}Ks2
暗号化
Ks2
1554
Ks2
Ks1発生
1552
1200
メモリ
インタフェース
メモリカード
130
音声再生
1112
キー
1108
ディスプレイ
1110
送受信
1104
コントローラ
1106
1102
バス
BS2

FIG. 8

FIG. 9

	記号	属性	特性	
メモリカード管理の鍵	Km	秘密復号鍵		メモリカード毎に異なる
	KPm	公開暗号鍵		KPmで暗号化されたデータは非対称な復号鍵Kmで復号可能
	Ks2	共通鍵	セッション固有	メモリと音楽再生モジュール間のアクセス毎に発生
音楽再生モジュール管理の鍵	Kp	秘密復号鍵	データ再生装置（携帯電話機）固有	データ再生装置毎に異なる
	Ks1	共通鍵	セッション固有	メモリと音楽再生モジュール間のアクセス毎に発生
配信データ	KPp	公開暗号鍵		KPpで暗号化されたデータは非対称な復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	コンテンツデータ		例：音楽データ

FIG. 10

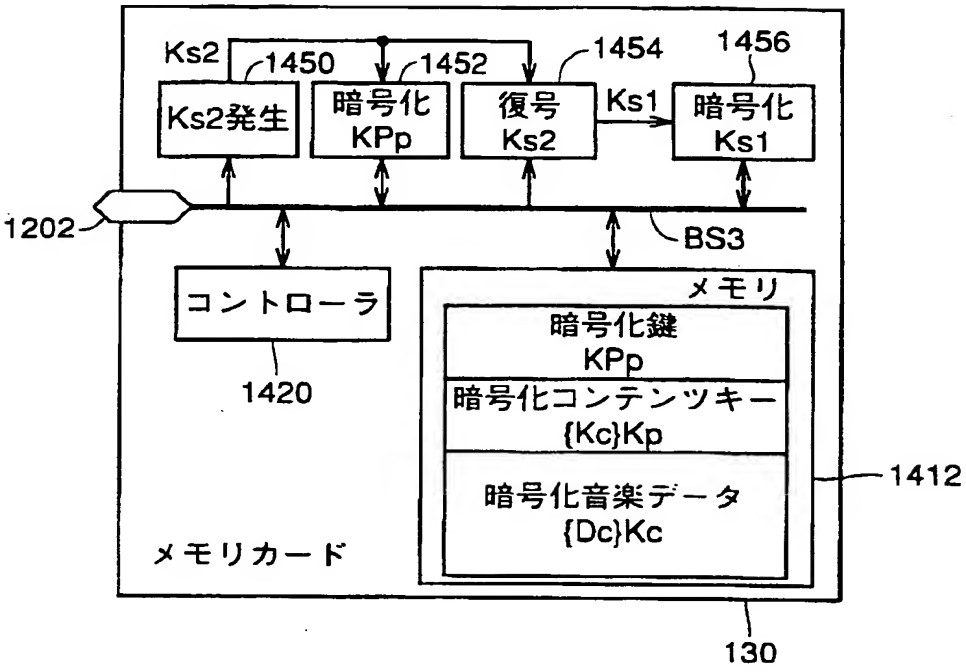

Ks2
1450
1452
1454
1456
Ks2発生
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
BS3
コントローラ
1420
メモリ
暗号化鍵
KPp
暗号化コンテンツキー
{Kc}Kp
暗号化音楽データ
{Dc}Kc
1412
メモリカード
130

FIG. 11

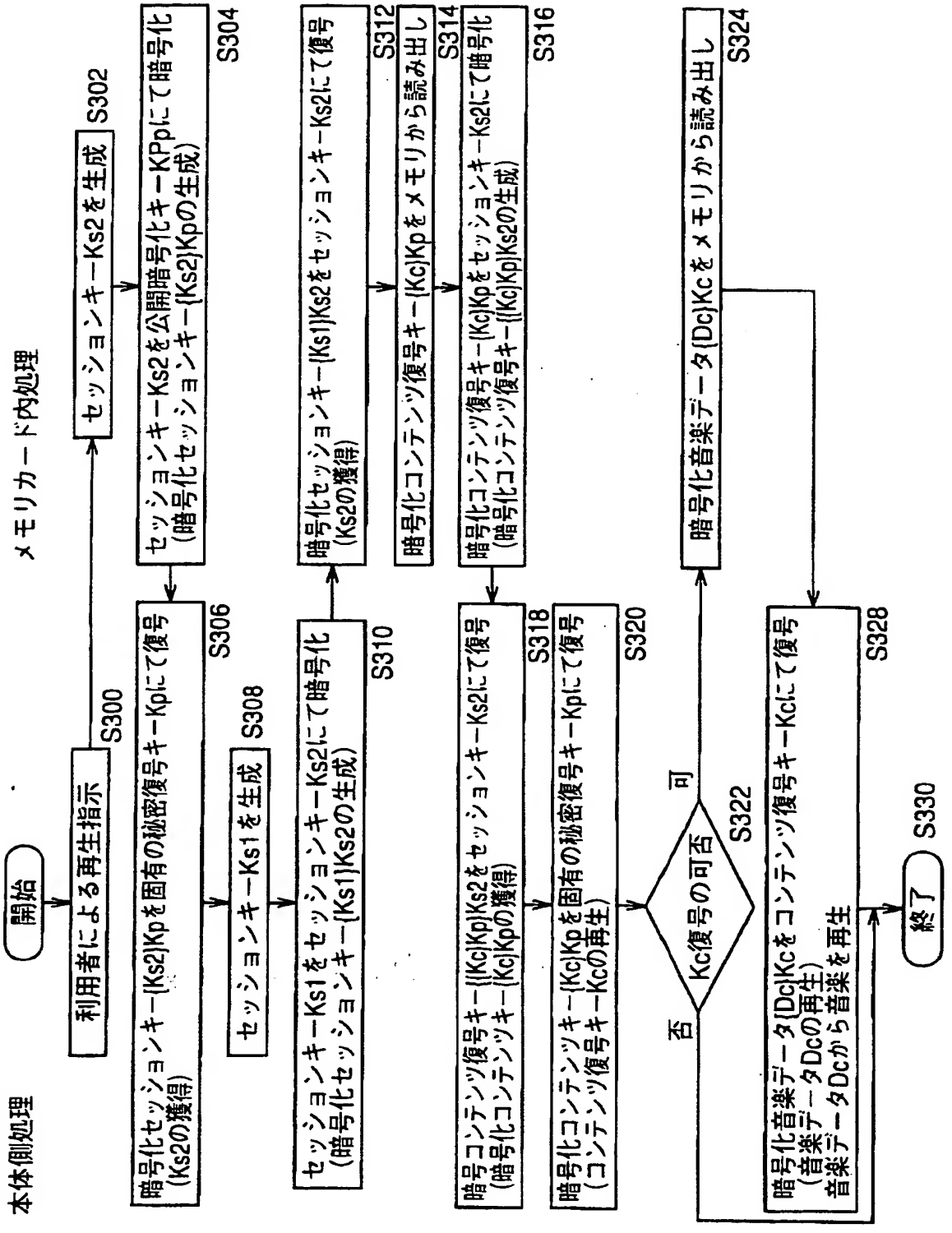

本体側処理
メモリカード内処理
開始
利用者による再生指示
S300
セッションキーKs2を生成
S302
暗号化セッションキー{Ks2}Kpを固有の秘密復号キーKpにて復号
(Ks2の獲得)
S306
セッションキーKs2を公開暗号化キーKPpにて暗号化
(暗号化セッションキー{Ks2}Kpの生成)
S304
セッションキーKs1を生成
S308
セッションキーKs1をセッションキーKs2にて暗号化
(暗号化セッションキー{Ks1}Ks2の生成)
S310
暗号化セッションキー{Ks1}Ks2をセッションキーKs2にて復号
(Ks2の獲得)
S312
暗号化コンテンツ復号キー{Kc}Kpをメモリから読み出し
S314
暗号コンテンツ復号キー{{Kc}Kp}Ks2をセッションキーKs2にて復号
(暗号化コンテンツ復号キー{Kc}Kpの獲得)
S318
暗号化コンテンツ復号キー{{Kc}Kp}Ks2をセッションキーKs2にて暗号化
(暗号化コンテンツ復号キー{{Kc}Kp}Ks2の生成)
S316
暗号化コンテンツ{Kc}Kpを固有の秘密復号キーKpにて復号
(コンテンツ復号キーKcの再生)
S320
Kc復号の可否
S322
否
可
暗号化音楽データ{Dc}Kcをメモリから読み出し
S324
暗号化音楽データ{Dc}Kcをコンテンツ復号キーKcにて復号
(音楽データDcの再生)
音楽データDcから音楽を再生
S328
終了
S330

FIG. 12

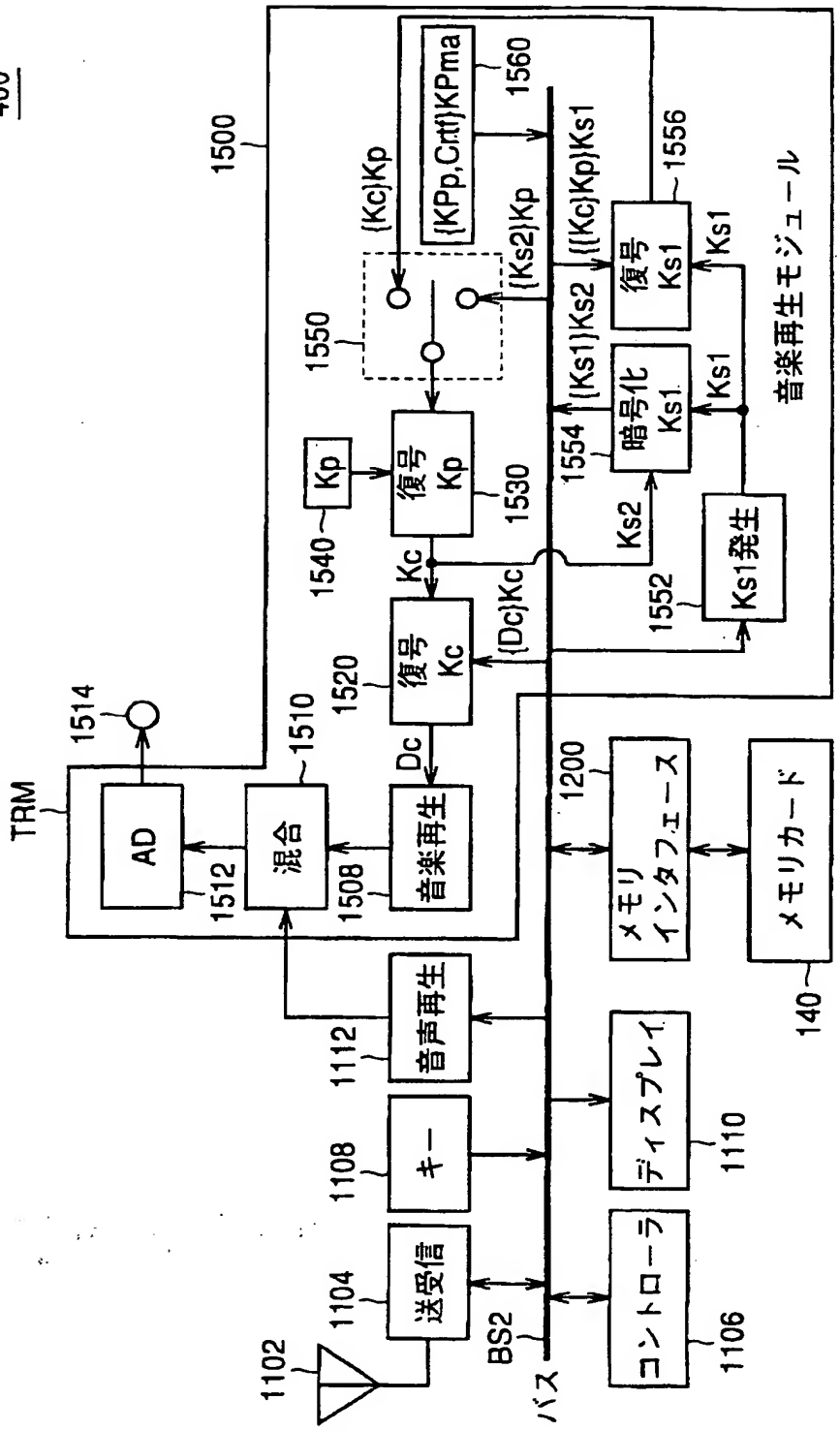

400
1500
TRM
1514
AD
1512
1510
混合
1508
音楽再生
1520
復号 Kc
Dc
Kc
1540
Kp
1530
復号 Kp
1550
{Kc}Kp
{KPp,Crtf}KPma
1560
{Ks2}Kp
{Dc}Kc
{Ks1}Ks2
{{Kc}Kp}Ks1
1554
暗号化 Ks1
1556
復号 Ks1
Ks1
Ks2
1552
Ks1発生
音楽再生モジュール
1200
メモリ インタフェース
メモリカード
140
音声再生
1112
キー
1108
ディスプレイ
1110
送受信
1104
コントローラ
1106
1102
BS2
バス

FIG. 13

	記号	属性	特性	
メモリカード管理の鍵	KPma	公開復号鍵	システム共通	(KPp,Crtf)KPmaの復号によってKPpの認証を行う機能を有する認証鍵
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール艦のアクセス毎に発生
音楽生成モジュール管理の鍵	KPp	公開暗号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

FIG. 14

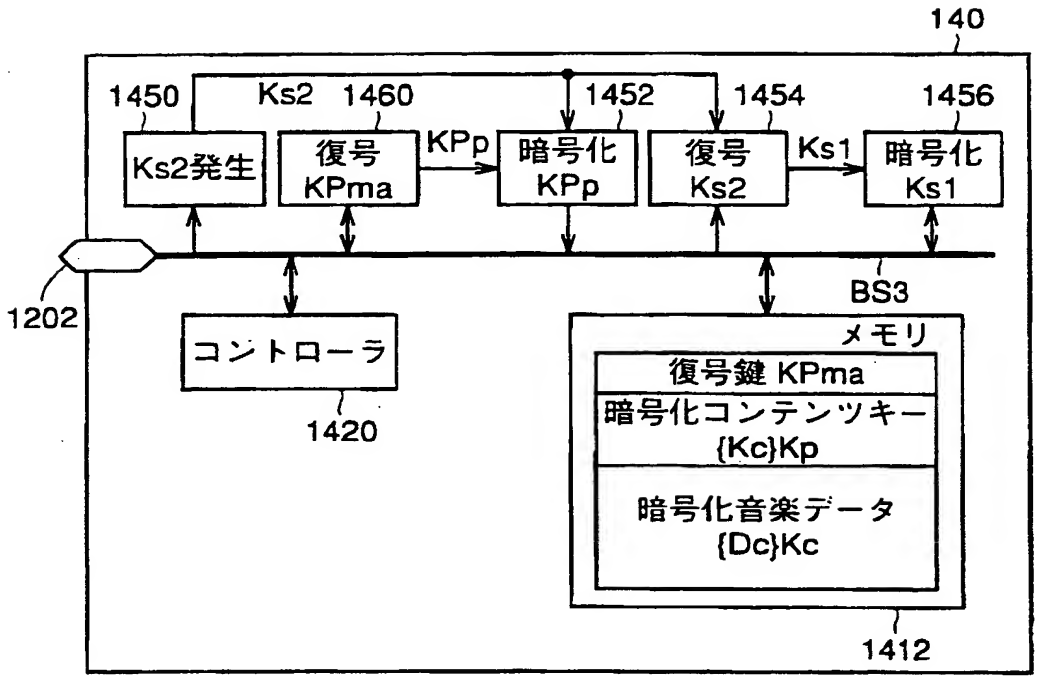

140
1450
Ks2
1460
1452
1454
1456
Ks2発生
復号
KPma
KPp
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
BS3
コントローラ
1420
メモリ
復号鍵 KPma
暗号化コンテンツキー
{Kc}Kp
暗号化音楽データ
{Dc}Kc
1412

FIG. 15

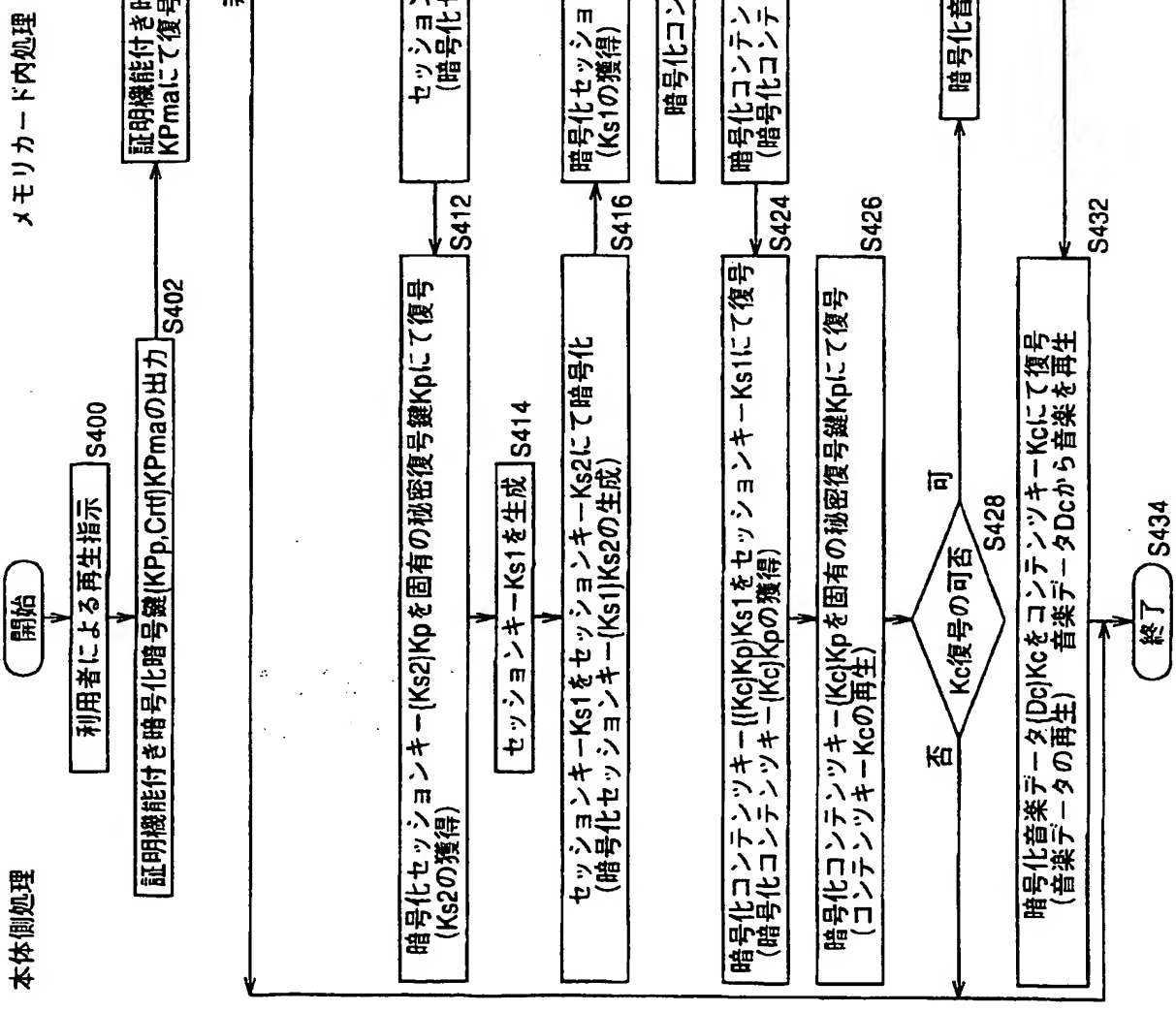

本体側処理
メモリカード内処理
開始
利用者による再生指示
S400
証明機能付き暗号化暗号鍵(KPp,Crtf)KPmaの出力
S402
証明機能付き暗号化暗号鍵(KPp,Crtf)KPmaを公開復号鍵KPmaにて復号（公開暗号鍵KPpの獲得）
S404
認証
S406
非承認
承認
セッションキーKs2を生成
S408
セッションキーKs1を公開暗号鍵KPpにて暗号化（暗号化セッションキー(Ks2)Kpの生成）
S410
暗号化セッションキー(Ks2)Kpを固有の秘密復号鍵Kpにて復号（Ks2の獲得）
S412
セッションキーKs1を生成
S414
セッションキーKs1をセッションキーKs2にて暗号化（暗号化セッションキー(Ks1)Ks2の生成）
S416
暗号化セッションキー(Ks1)Ks2をセッションキーKs2にて復号（Ks1の獲得）
S418
暗号化コンテンツキー(Kc)Kpをメモリから読み出し
S420
暗号化コンテンツキー(Kc)Kpをセッションキーks1にて暗号化（暗号化コンテンツキー{(Kc)Kp}Ks1の生成）
S422
暗号化コンテンツキー{(Kc)Kp}Ks1をセッションキーKs1にて復号（暗号化コンテンツキー(Kc)Kpの獲得）
S424
暗号化コンテンツキー(Kc)Kpを固有の秘密復号鍵Kpにて復号（コンテンツキーKcの再生）
S426
Kc復号の可否
S428
否
可
暗号化音楽データ(Dc)Kcをメモリから読み出し
S430
暗号化音楽データ(Dc)Kcをコンテンツキー Kcにて復号（音楽データの再生）音楽データDcから音楽を再生
S432
終了
S434

FIG. 16

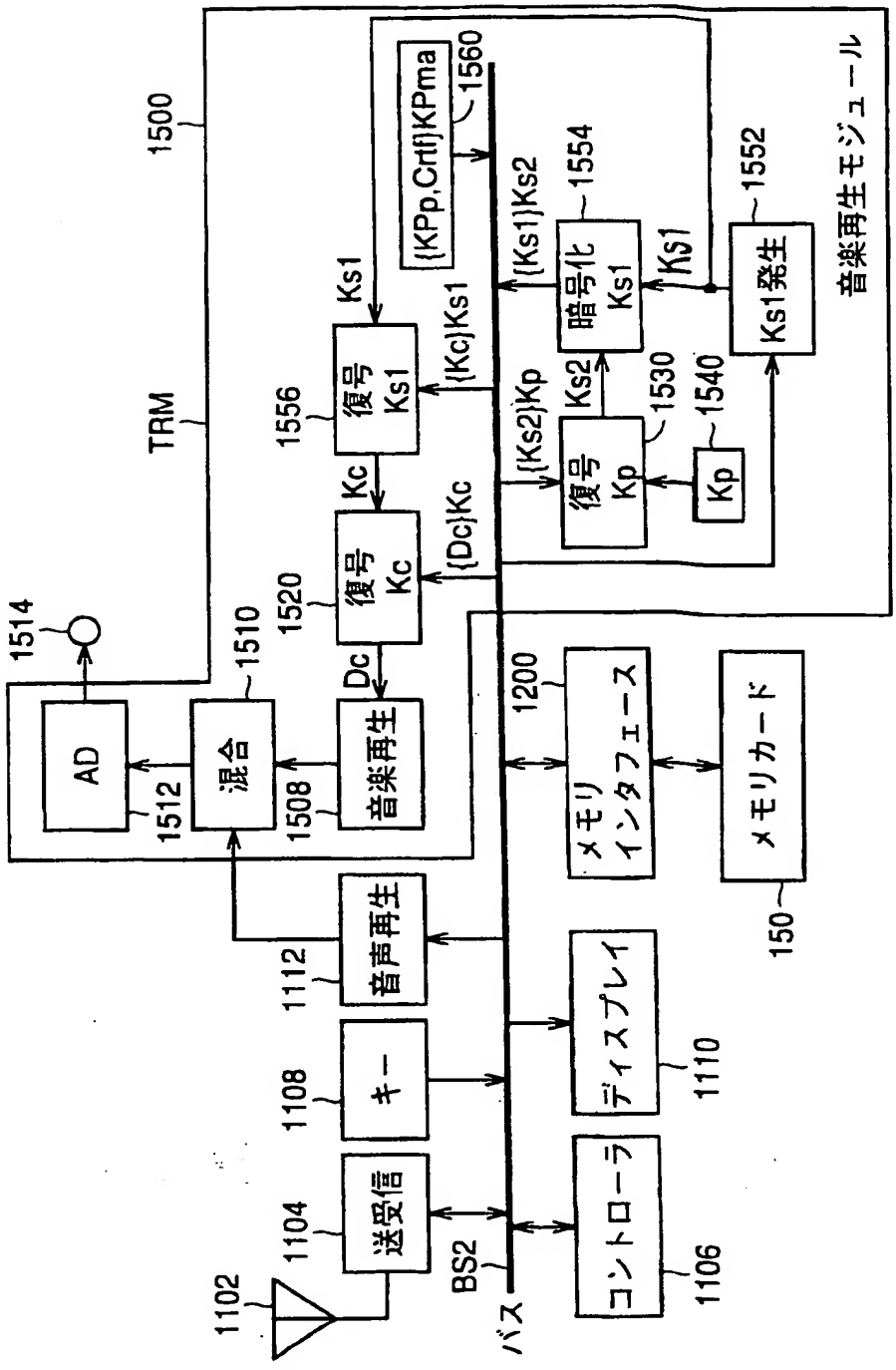

500
1500
TRM
音楽再生モジュール
1514
AD
1512
1510
混合
1508
音楽再生
1520
復号 Kc
Dc
Kc
1556
復号 Ks1
Ks1
{KPp,Crtf}KPma
1560
{Kc}Ks1
{Dc}Kc
{Ks1}Ks2
1554
暗号化 Ks1
Ks1
1552
Ks1発生
{Ks2}Kp
Ks2
復号 Kp
1530
Kp
1540
1200
メモリインタフェース
メモリカード
150
1102
1104
送受信
BS2
1108
キー
1112
音声再生
ディスプレイ
1110
コントローラ
1106
バス

FIG. 17

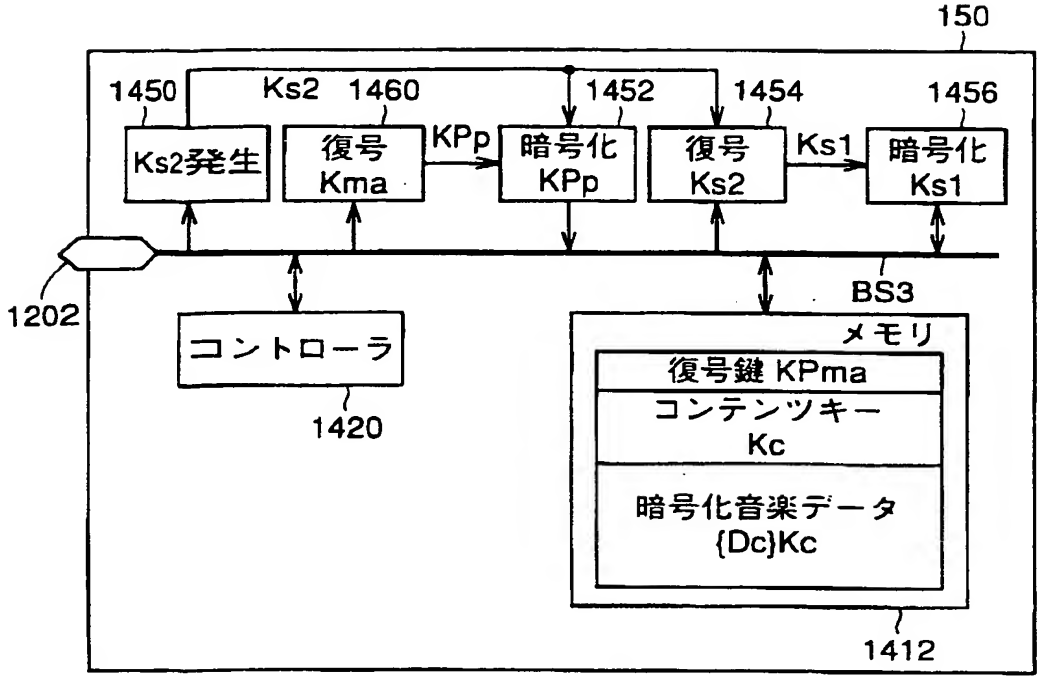

150
1450
Ks2
1460
1452
1454
1456
Ks2発生
復号
Kma
KPp
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
BS3
コントローラ
1420
メモリ
復号鍵 KPma
コンテンツキー
Kc
暗号化音楽データ
{Dc}Kc
1412

FIG. 18

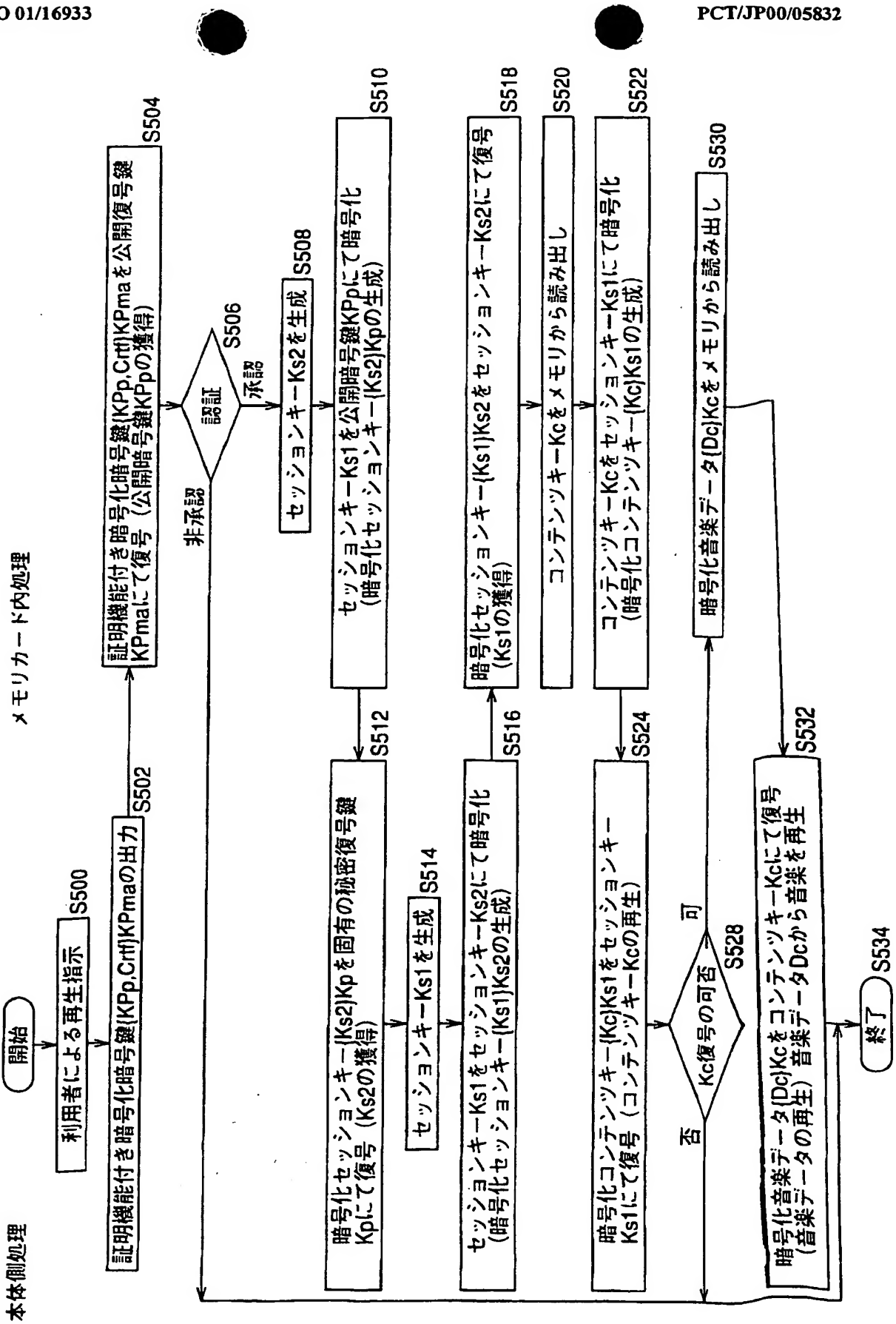

本体側処理
メモリカード内処理
開始
利用者による再生指示
S500
証明機能付き暗号化暗号鍵{KPp,Crtf}KPmaの出力
S502
証明機能付き暗号化暗号鍵{KPp,Crtf}KPmaを公開復号鍵KPmaにて復号（公開暗号鍵KPpの獲得）
S504
認証
S506
非承認
承認
セッションキーKs2を生成
S508
セッションキーKs1を公開暗号鍵KPpにて暗号化
（暗号化セッションキー{Ks2}Kpの生成）
S510
暗号化セッションキー{Ks2}Kpを固有の秘密復号鍵Kpにて復号（Ks2の獲得）
S512
セッションキーKs1を生成
S514
セッションキーKs1をセッションキーKs2にて暗号化
（暗号化セッションキー{Ks1}Ks2の生成）
S516
暗号化セッションキー{Ks1}Ks2をセッションキーKs2にて復号
（Ks1の獲得）
S518
コンテンツキーKcをメモリから読み出し
S520
コンテンツキーKcをセッションキーKs1にて暗号化
（暗号化コンテンツキー{Kc}Ks1の生成）
S522
暗号化音楽データ{Dc}Kcをメモリから読み出し
S530
暗号化コンテンツキー{Kc}Ks1をセッションキーKs1にて復号（コンテンツキーKcの再生）
S524
Kc復号の可否
S528
否
可
暗号化音楽データ{Dc}Kcをコンテンツキー Kcにて復号
（音楽データの再生）音楽データDcから音楽を再生
S532
終了
S534

FIG. 19

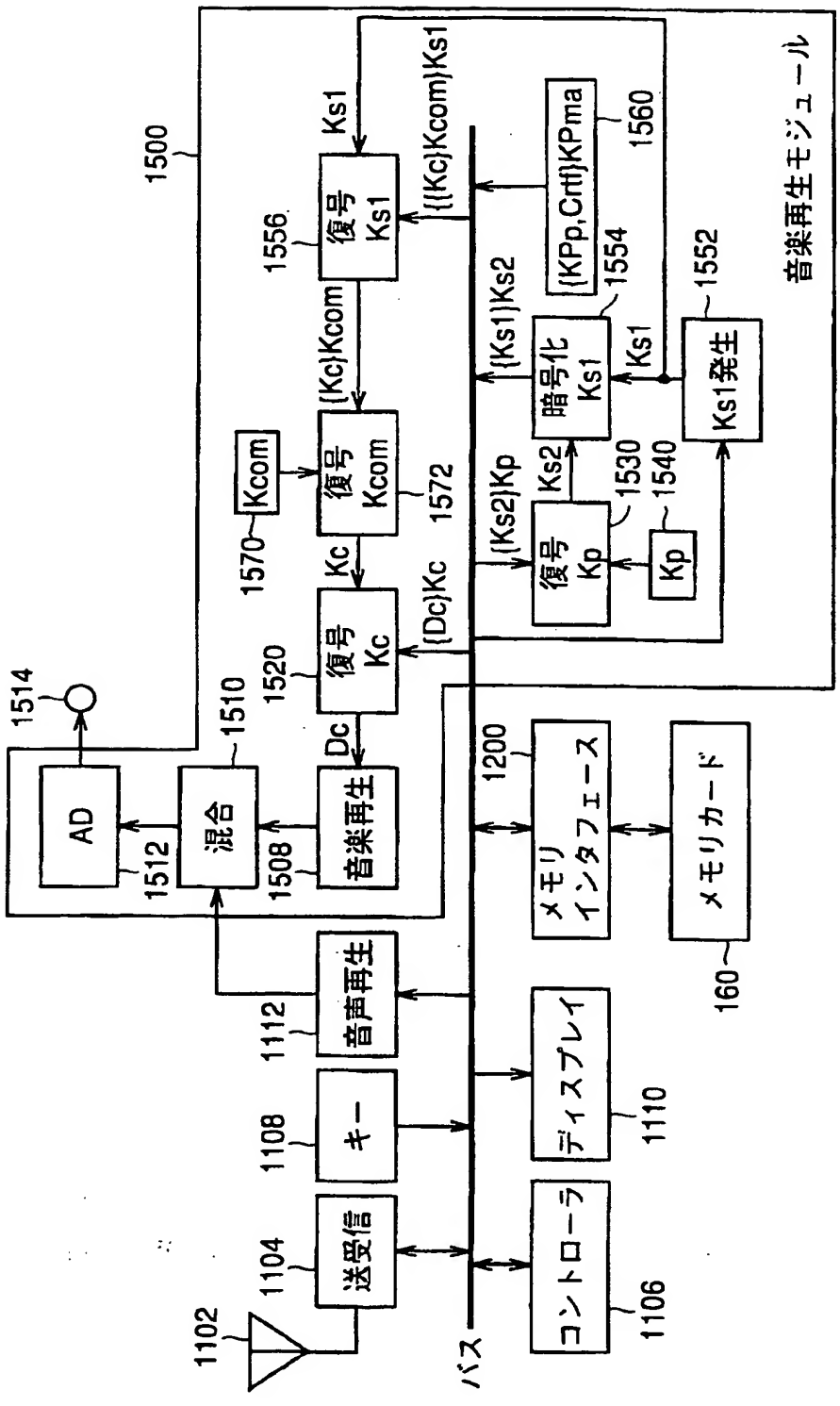

600
1500
音楽再生モジュール
1514
AD
1512
1510
混合
1508
1520
音楽再生
Dc
復号
Kc
Kc
1572
復号
Kcom
Kcom
1570
{Kc}Kcom
1556
復号
Ks1
Ks1
{{Kc}Kcom}Ks1
{Dc}Kc
{Ks2}Kp
復号
Kp
Ks2
1530
1540
Kp
{Ks1}Ks2
暗号化
Ks1
Ks1
1554
{KPp,Crtl}KPma
1560
Ks1発生
1552
1200
メモリ
インタフェース
メモリカード
160
1112
音声再生
1108
キー
ディスプレイ
1110
1104
送受信
コントローラ
1106
1102
バス

FIG. 20

	記号	属性	特性	
メモリカード管理の鍵	KPma	公開復号鍵	システム共通	{KPp}KPmaの復号によってKPpの認証を行う機能を有する認証鍵
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール艦のアクセス毎に発生
音楽生成モジュール管理の鍵	KPp	公開暗号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Kcom	秘密復号鍵	システム共通	暗号化されたコンテンツキーを復号する
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

FIG. 21

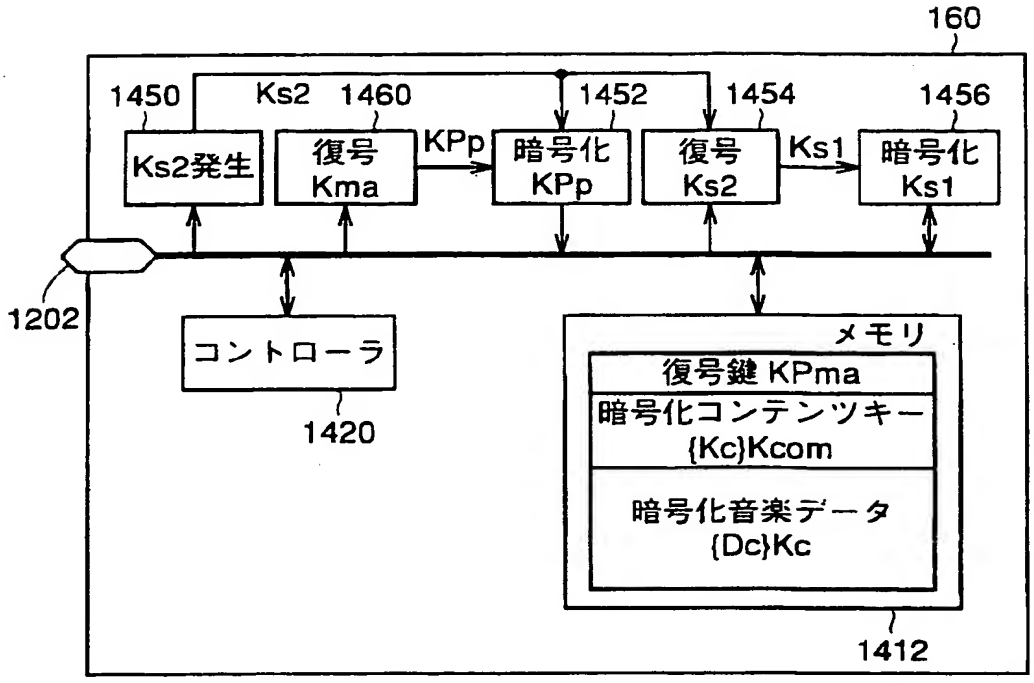
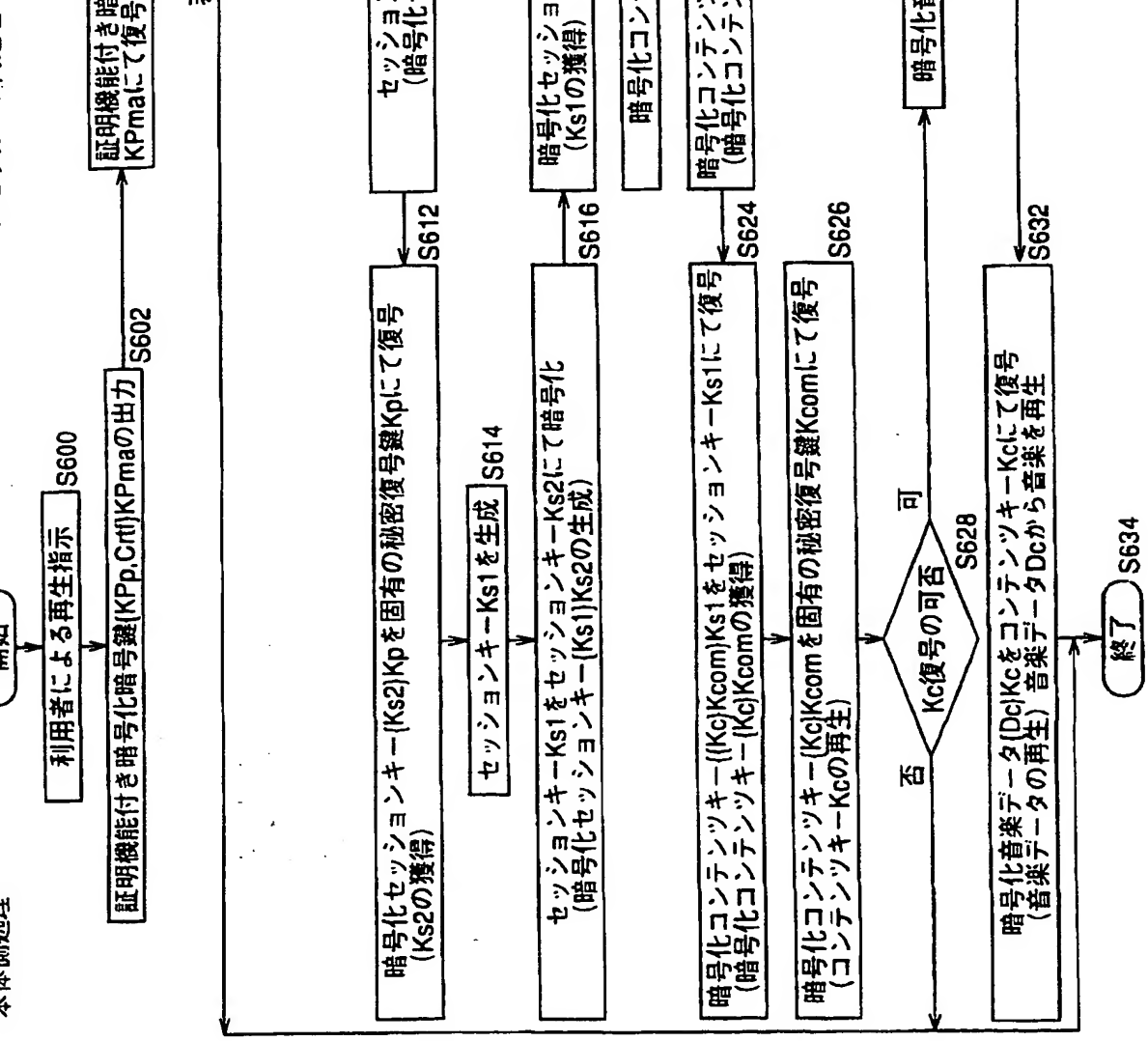

160
1450
Ks2
1460
1452
1454
1456
Ks2発生
復号
Kma
KPp
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
コントローラ
1420
メモリ
復号鍵 KPma
暗号化コンテンツキー
{Kc}Kcom
暗号化音楽データ
{Dc}Kc
1412

FIG. 22


本体側処理
メモリカード内処理
開始
利用者による再生指示
S600
証明機能付き暗号化暗号鍵(KPp,Crt)KPmaの出力
S602
証明機能付き暗号鍵(KPp,Crt)KPmaを公開復号鍵KPmaにて復号（公開暗号鍵KPpの獲得）
S604
認証
S606
承認
非承認
セッションキーKs2を生成
S608
セッションキーKs1を公開暗号鍵KPpにて暗号化（暗号化セッションキー(Ks2)Kpの生成）
S610
暗号化セッションキー(Ks2)Kpを固有の秘密復号鍵Kpにて復号（Ks2の獲得）
S612
セッションキーKs1を生成
S614
セッションキーKs1をセッションキーKs2にて暗号化（暗号化セッションキー(Ks1)Ks2の生成）
S616
暗号化セッションキー(Ks1)Ks2をセッションキーKs2にて復号（Ks1の獲得）
S618
暗号化コンテンツキー(Kc)Kcomをメモリから読み出し
S620
暗号化コンテンツキー(Kc)Kcomをセッションキーks1にて暗号化（暗号化コンテンツキー{(Kc)Kcom}Ks1の生成）
S622
暗号化コンテンツキー{(Kc)Kcom}Ks1をセッションキーKs1にて復号（暗号化コンテンツキー(Kc)Kcomの獲得）
S624
暗号化コンテンツキー(Kc)Kcomを固有の秘密復号鍵Kcomにて復号（コンテンツキーKcの再生）
S626
Kc復号の可否
S628
否
可
暗号化音楽データ(Dc)Kcをメモリから読み出し
S630
暗号化音楽データ(Dc)Kcをコンテンツキー Kcにて復号（音楽データの再生）音楽データDcから音楽を再生
S632
終了
S634

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05832

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10, G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08, G10L19/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G10K15/00-15/06, G10L19/00-19/14, H04L9/00-9/38, G09C1/00-5/00, G06F12/00, G06F12/14, H04M11/00-11/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1995 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
INSPEC (DIALOG)
WPI (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP, 817185, A2 (Kabushiki Kaisha TOSHIBA), 07 January, 1998 (07.01.98), Full text, all drawings & JP, 10-106148, A & JP, 3093678, B2 & TW, 340920, A & KR, 98086354, A & CN, 1183685, A	1 2-22
X Y	JP, 9-326166, A (Mitsubishi Electric Corporation), 16 December, 1997 (16.12.97), Full text, all drawings (Family: none)	1 2-22
Y	JP, 10-40172, A (Toshiba Corporation), 13 February, 1998 (13.02.98), Full text, all drawings (Family: none)	2-22
Y	Nikkei Electronics, No.739, "Kagata Memory Card de Ongaku Chosakuken wo mamoru", 22 March, 1999 (22.03.99), pp.49-53	2-22
Y	Nikkei Electronics, No.728, "Bei Shuuhen Kiki Maker Ootega, MP3 Keitaigata Player Hatsubai; Chosakuken taisaku ha Fuka sezu",	2-22

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 November, 2000 (10.11.00)	21 November, 2000 (21.11.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05832

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	19 October, 1998 (19.10.98), pp.31-32	
A	Nikkei Electronics, No.731, "Yogoreta Image Fusshoku Nerau MP3 Gyoukai; Ongaku Haishin no Kaigi 'Web noise' kara", 30 November,1998 (30.11.98), pp.29-30	1-22

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５８３２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int Cl' Ｇ１０Ｋ１５／０２，Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１７／６０，Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／１０，
Ｇ０６Ｋ１９／００，Ｈ０４Ｈ１／００，Ｈ０４Ｍ３／４２，Ｈ０４Ｍ３／４９３，Ｈ０４Ｍ１１／０８，
Ｇ１０Ｌ１９／００

Ｂ．　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int Cl' Ｇ１０Ｋ１５／００～１５／０６，Ｇ１０Ｌ１９／００～１９／１４，Ｈ０４Ｌ９／００～９／３８，
Ｇ０９Ｃ１／００～５／００，Ｇ０６Ｆ１２／００，Ｇ０６Ｆ１２／１４，Ｈ０４Ｍ１１／００～１１／１０

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２６～１９９５年
日本国公開実用新案公報　１９７１～２０００年
日本国登録実用新案公報　１９９４～２０００年
日本国実用新案登録公報　１９９６～２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）
ＷＰＩ（ＤＩＡＬＯＧ）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＥＰ，８１７１８５，Ａ２(Kabushiki kaisha TOSHIBA) 7.1月.1998(07.01.98)，全文全図， &JP,10-106148,A &JP,3093678,B2 &TW,340920,A &KR,98086354,A &CN,1183685,A	1
Ｙ		2-22
Ｘ	ＪＰ，９－３２６１６６，Ａ(三菱電機株式会社) 16.12月.1997(16.12.97)，全文全図，（ファミリーなし）	1
Ｙ		2-22

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１０．１１．００	21.11.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	松尾　淳一　印	５Ｃ　８８４２
	電話番号　０３－３５８１－１１０１　内線　３５４０	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５８３２

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，１０－４０１７２，Ａ(株式会社東芝) 13.2月.1998(13.2.98)，全文全図，（ファミリーなし）	2-22
Ｙ	日経エレクトロニクス，No.739，「小型メモリ・カードで音楽著作権を守る」，22.3月.1999(22.03.99)，p.49-53	2-22
Ｙ	日経エレクトロニクス，No.728，「米周辺機器メーカ大手が，ＭＰ３携帯型プレーヤ発売　著作権対策は付加せず」， 19.10月.1998(19.10.98)，p.31-32	2-22
Ａ	日経エレクトロニクス，No.731，「汚れたイメージ払拭ねらうＭＰ３業界 音楽配信の会議 Webnoise から」， 30.11月.1998(30.11.98)，p.29-30	1-22